UNIVERSIDAD LATINOAMERICANA DE CIENCIA Y TECNOLÓGIA.

ULACIT

Escuela de Ingeniería Informática.

ARTÍCULO CIENTÍFICO

Seguridad biométrica: Análisis de los sistemas de biometría actual.

Autor : Alberto López Morales.
Ced : 8-074-123
albertolm@costarricense.cr

Prof. Miguel Pérez Montero

23/08/2005

INDICE

Seguridad Biométrica: Un análisis de la biometría actual.

Autor: Alberto López Morales.

.

· Bachiller en Ingeniería Informática. Candidato a Licenciatura en Ingeniería Informática con énfasis en Telemática, ULACIT. Correo electrónico: albertolm@costarricense.cr

Dedicatoria.

Dedico a este material a todas aquellas personas que luchan por obtener excelentes resultados en todas las buenas obras que realicen por simples que estas sean catalogadas.

Agradecimientos.

Noble agradecimiento a profesor guía, compañeros de Universidad y amistades que colaboraron conmigo a recopilar datos necesarios para llevar a cabo este producto. Principalmente infinitas gracias a Dios por darme la oportunidad de poder expresarme para bien.

Resumen:

La seguridad a nivel mundial y en todos los esquemas representa una de las variables principales y de prioridad, sin embargo en estos últimos años a partir de la tragedia del 11 de septiembre del 2002 ocurrida en New York y Washington, se ha incrementado la necesidad de reforzar la seguridad en lugares de acceso controlado como oficinas gubernamentales, aeropuertos, hospitales con el uso de dispositivos Biométricos, que tienen la capacidad de verificar automáticamente la identidad de las personas basándose en características físicas como huellas digitales, simetría del rostro, iris, retina ocular o del comportamiento individual de las personas como voz y firma. La mayoría funcionan de manera muy similar, consistiendo en que la persona debe ser registrada en el sistema, capturando el rasgo característico de ella, creando así uno o varios modelos de referencia y guardado en una base de datos. Para realizar una verificación de identidad de una persona, el sistema captura el rasgo característico y lo compara con el o los modelos de referencia antes almacenados en la base de datos, resultando exitosa si la comparación es acertada, entonces se conceden los privilegios, de lo contrario los privilegios son negados.

Abstract.

The security at world level and in all the outlines one of the main variables represents and of priority, however in these last years starting from the tragedy of September 11 the 2002 happened in New York and Washington, the necessity has been increased of reinforcing the security in places of controlled access like government offices, airports, hospitals with the use of devices Biométricos that have the capacity to verify the identity of people automatically being based on physical characteristics how fingerprints, symmetry of the face, iris, ocular retina or of the individual behavior of people how voice, it signs. Most works in a very similar way, consisting in that the person should be registered in the system, capturing the characteristic feature of her, creating this way one or several reference models and kept in a database. To carry out a verification of a person's identity, the system captures the characteristic feature and it compares it before with him or the reference models stored in the database, being successful if the comparison is guessed right, then the privileges are granted, otherwise the privileges are denied.

Compendio:

Palabras clave: biometría, seguridad, protección, reconocimiento, huellas.

En estos últimos tiempos, el factor seguridad ha sido una variable de primera mano en todas las actividades cotidianas, y se han perseguido varias formas mantener estos niveles de seguridad en los puntos más altos que permitan de mantener cierto grado de tranquilidad y menos riesgos catastróficos sin embargo, en la medida que se van inventando o desarrollando medidas o sistemas de seguridad "más seguros" se irán creando casi paralelamente sistemas o artimañas que valgan para violar estas innovaciones, mientras se siguen buscando otras herramientas que superen y contrarresten todas esas debilidades que los anteriores sistemas poseían. En este artículo se dan a conocer ciertos niveles y dispositivos de seguridad que están tomando auge en estos últimos días dada la cantidad de amenazas de todo tipo en las que el mundo se encuentra inmerso. Los sistemas tecnológicos han venido desarrollando y mejorando sistemas de seguridad tratando de mantener a salvo todo aquello que se considere de utilidad y de acceso restringido solo para usuarios determinados eso en lo que respecta a datos y controles de acceso sin embargo estos sistemas permiten obtener una mejor administración de usuarios, clientes, sistemas de computadores y sobre todo determinar "quien es quien".

Este artículo se desarrolla basándose en investigación, lecturas y revisiones de otras fuentes de revistas, accesos a bases de datos de EBSCO con artículos afines, así como entrevistas en algunas empresas que hacen uso de esta tecnología. Su estructura se conforma desde la necesidad de seguridad analizando los factores que llevan a cabo la motivación al desarrollo de esta tecnología más confiable a consecuencia de los ataques hacia los sistemas de información que se viven actualmente, tampoco se pretende establecer que es la cura para este tipo de males, pues habrá sistemas con niveles de seguridad más altos unos que otros, así como los más aplicados, también se describen las características y funcionamiento de cada uno de ellos, se verán recomendaciones para aplicar de acuerdo a las experiencias de muchos usuarios.

Lógicamente esta tecnología biométrica se reforzará conforme las violaciones se vayan haciendo más evidentes sin dejar a un lado las otras aplicaciones comerciales que se interpondrán.

Necesidad de Seguridad.

¿Qué es seguridad?

Se puede entender como seguridad una característica de cualquier sistema (informático o no) que indica que ese sistema está libre de todo peligro, daño o riesgo, y que es, en cierta manera, infalible. Como esta característica, particularizando para el caso de sistemas operativos o redes de computadores, es muy difícil de conseguir (según la mayoría de expertos, imposible), se suaviza la definición de seguridad y se pasa a hablar de fiabilidad (probabilidad de que un sistema se comporte tal y como se espera de él) más que de seguridad; Por tanto, se habla de sistemas fiables en lugar de hacerlo de sistemas seguros. (Villalón,2002)

A grandes rasgos se entiende que mantener un sistema seguro (o fiable) consiste básicamente en garantizar tres aspectos: confidencialidad, integridad y disponibilidad. Algunos estudios integran la seguridad dentro de una propiedad más general de los sistemas, la confiabilidad, entendida como el nivel de calidad del servicio ofrecido. Consideran la disponibilidad como un aspecto al mismo nivel que la seguridad y no como parte de ella, por lo que dividen esta última en sólo las dos facetas restantes, confidencialidad e integridad. En este trabajo no seguiremos esa corriente por considerarla minoritaria.

¿Por qué preocupa la seguridad?

- A partir de los años 80 el uso del ordenador personal comienza a ser común. Asoma ya la preocupación por la integridad de los datos.
- En la década de los años 90 proliferan los ataques a sistemas informáticos, aparecen los virus y se toma conciencia del peligro que acecha a usuarios de PCs y equipos conectados a Internet.
- Las amenazas se generalizan a finales de los 90.

¿Qué hay de nuevo en los años 2000 ?

Principalmente por el uso de Internet, el tema de la protección de la información se transforma en una necesidad y con ello se populariza la terminología “Políticas de seguridad”:

– Normas, recomendaciones, estándares.

– Protección de la información

- El usuario final desea saber, por ejemplo, como evitar los virus en un e-mail.
- Productos futuros: Seguridad añadida.

Qué se debe proteger?

Los tres elementos principales a proteger en cualquier sistema informático son el software, el hardware y los datos.

Habitualmente los datos constituyen el principal elemento de los tres a proteger, ya que es el más amenazado y seguramente el más difícil de recuperar. Sin embargo, en caso de pérdida de una base de datos o de un proyecto de un usuario, se tiene un medio original desde el que restaurar: se ha de pasar obligatoriamente por un sistema de copias de seguridad, y a menos que la política de copias sea muy estricta, es difícil devolver los datos al estado en que se encontraban antes de la pérdida.

Contra cualquiera de los tres elementos mencionados anteriormente (pero principalmente sobre los datos) se pueden realizar multitud de ataques o, dicho de otra forma, están expuestos a diferentes amenazas. Generalmente, la clasificación más elemental de estas amenazas las divide en cuatro grandes grupos: interrupción, interceptación, modificación y fabricación. Un ataque se clasifica como interrupción si hace que un objeto del sistema se pierda, quede inutilizable o no disponible. Se tratará de una interceptación si un elemento no autorizado consigue un acceso a un determinado objeto del sistema, y de una modificación si además de conseguir el acceso consigue modificar el objeto; algunos autores consideran un caso especial de la modificación: la destrucción, entendiéndola como una modificación que inutiliza al objeto afectado. Por último, se dice que un ataque es una fabricación si se trata de una modificación destinada a conseguir un objeto similar al atacado de forma que sea difícil distinguir entre el objeto original y el 'fabricado' o 'generado'.

Amenazas de interrupción. (Villalón, 2002)

- Se daña, pierde o deja de funcionar un punto del sistema.
- Detección inmediata. Ejemplos: Destrucción del hardware, Borrado de programas, datos, Fallos en el sistema operativo.

Amenazas de interceptación.

- Acceso a la información por parte de personas no autorizadas. Uso de privilegios no adquiridos.
- Detección difícil, no dejar huellas. Ejemplos: Copias ilícitas de programas, escuchar en línea de datos.

Amenazas de modificación.

- Acceso no autorizado que cambia el entorno para su beneficio.
- Detección difícil según circunstancias. Ejemplos: Modificación de bases de datos, Modificación de elementos del Hardware.

Amenazas de fabricación o generación

- Creación de nuevos objetos dentro del sistema.
- Detección difícil. Delitos de falsificación. Ejemplos: Añadir transacciones en red, Añadir registros en base de datos.

De qué se quiere proteger?

Con frecuencia, especialmente en las obras menos técnicas y más orientadas a otros aspectos de la seguridad se suele identificar a los atacantes únicamente como personas; esto tiene sentido si se habla por ejemplo de responsabilidades por un delito informático. Pero en este trabajo es preferible hablar de `elementos' y no de personas: aunque a veces se olvide, algunos sistemas pueden verse perjudicados por múltiples entidades aparte de humanos, como por ejemplo programas, catástrofes; si un usuario pierde un trabajo importante a causa de un ataque, poco le importará que haya sido un intruso, un gusano, un simple error del administrador, etc.

A continuación se presenta una relación de los elementos que potencialmente pueden amenazar a los sistemas.

Personas

Es una Realidad : la mayoría de ataques a los sistemas van a provenir en última instancia de personas que, intencionada o inintencionadamente, pueden causar enormes pérdidas. Generalmente se tratará de piratas que intentan conseguir el máximo nivel de privilegio posible aprovechando alguno (o algunos) de los riesgos lógicos de los que se hablaran a continuación, especialmente agujeros del software. Pero con demasiada frecuencia se suele olvidar que los piratas `clásicos' no son los únicos que amenazan los equipos: es especialmente preocupante que mientras que hoy en día cualquier administrador mínimamente preocupado por la seguridad va a conseguir un sistema relativamente fiable de una forma lógica (permaneciendo atento a vulnerabilidades de su software, restringiendo servicios, utilizando cifrado de datos...), pocos administradores tienen en cuenta factores como la ingeniería social a la hora de diseñar una política de seguridad.

Aquí se describen brevemente los diferentes tipos de personas que de una u otra forma pueden constituir un riesgo para los sistemas; generalmente se dividen en dos grandes grupos: los atacantes pasivos, aquellos que fisgonean por el sistema pero no lo modifican -o destruyen-, y los activos, aquellos que dañan el objetivo atacado, o lo modifican en su favor. Generalmente los curiosos y los crackers realizan ataques pasivos (que se pueden convertir en activos), mientras que los terroristas y ex-empleados realizan ataques activos puros; los intrusos remunerados suelen ser atacantes pasivos si la red o equipo no es su objetivo, y activos en caso contrario, y el personal realiza ambos tipos indistintamente, dependiendo de la situación concreta.

Curiosos

Al igual que los crackers, los curiosos son los atacantes más habituales de sistemas y es de recordar que también las personas suelen ser curiosas por naturaleza; por lo tanto, habrá personal intentando conseguir mayor privilegio del que tienen o intentando acceder a sistemas a los que oficialmente no tienen acceso. Ya sea para comprobar que es posible romper la seguridad de un sistema concreto.

Crackers

Los entornos de seguridad media son un objetivo típico de los intrusos, ya sea para fisgonear, para utilizarlas como enlace hacia otras redes o simplemente por diversión. Por un lado, son redes generalmente abiertas, y la seguridad no es un factor tenido muy en cuenta en ellas; esto convierte a las empresas , en un objetivo fácil y apetecible para piratas con cualquier nivel de conocimientos, desde los más novatos (y a veces más peligrosos) hasta los expertos, que pueden utilizar toda la red para probar nuevos ataques o como nodo intermedio en un ataque a otros organismos, con el consiguiente deterioro de imagen (y a veces de presupuesto)

Terroristas

Un `terrorista' se engloba a cualquier persona que ataca al sistema simplemente por causar algún tipo de daño en él. Por ejemplo, alguien puede intentar borrar las bases de datos. o destruir los sistemas de archivos de un servidor que alberga páginas web.

Este es el grupo de atacantes de un sistema más peligroso, aunque por fortuna el menos habitual en redes normales; suele afectar más a las grandes empresas o a organismos de defensa. Se trata de personas con gran experiencia en problemas de seguridad y un amplio conocimiento del sistema, que son pagados por terceros, generalmente para robar secretos. (una base de datos de clientes, información confidencial sobre algunas tácticas militares, etc) o simplemente para dañar la imagen de la entidad afectada.

Personal Interno

Las amenazas a la seguridad de un sistema provenientes del personal de la propia organización rara vez son tomadas en cuenta; se presupone un entorno de confianza donde a veces no existe, por lo que se pasa por alto el hecho de que casi cualquier persona de la organización, incluso el personal ajeno a la infraestructura informática (secretariado, personal de seguridad, personal de limpieza y mantenimiento...) puede comprometer la seguridad de los equipos.

Aunque los ataques pueden ser intencionados (en cuyo caso sus efectos son extremadamente dañinos, recordemos que nadie mejor que el propio personal de la organización conoce mejor los sistemas...y sus debilidades), lo normal es que más que de

ataques se trate de accidentes causados por un error o por desconocimiento2.4 de las normas básicas de seguridad.

Ex-empleados

Otro gran grupo de personas potencialmente que no se descartan en atacar un sistema son los antiguos empleados de la misma institución, especialmente los que no abandonaron el entorno por voluntad propia (y en el caso de redes de empresas, los que pasaron a la competencia). Generalmente, se trata de personas descontentas con la organización que pueden aprovechar debilidades de un sistema que conocen perfectamente para dañarlo como venganza por algún hecho que no consideran justo: amparados en excusas como `No me han pagado lo que me deben' o `Es una gran Entidad, se lo pueden permitir' pueden insertar troyanos, virus...o simplemente conectarse al sistema como si aún trabajaran para la organización (muchas veces se mantienen las cuentas abiertas incluso meses después de abandonar la institución).

Amenazas lógicas

Bajo la etiqueta de `amenazas lógicas' se encuentran todo tipo de programas que de una forma u otra pueden dañar a un sistema, creados de forma intencionada para ello (software malicioso, también conocido como malware) o simplemente por error (*bugs* o agujeros).

Herramientas de seguridad

Cualquier herramienta de seguridad representa un arma de doble filo: de la misma forma que un administrador las utiliza para detectar y solucionar fallos en sus sistemas o en la subred completa, un potencial intruso las puede utilizar para detectar esos mismos fallos y aprovecharlos para atacar los equipos.

Puertas traseras

Durante el desarrollo de aplicaciones grandes o de sistemas operativos es habitual entre los programadores insertar `atajos' en los sistemas habituales de autenticación del programa o del núcleo que se está diseñando. A estos atajos se les denomina puertas traseras, y con ellos se consigue mayor velocidad a la hora de detectar y depurar fallos: por ejemplo, los diseñadores de un software de gestión de bases de datos en el que para acceder a una tabla

se necesiten cuatro claves diferentes de diez caracteres cada una pueden insertar una rutina para conseguir ese acceso mediante una única clave `especial', con el objetivo de perder menos tiempo al depurar el sistema.

Algunos programadores pueden dejar estos atajos en las versiones definitivas de su software para facilitar un mantenimiento posterior, para garantizar su propio acceso, o simplemente por descuido; la cuestión es que si un atacante descubre una de estas puertas traseras (no importa el método que se utilice para hacerlo) va a tener un acceso global a datos que no debería poder leer, lo que obviamente supone un grave peligro para la integridad de un sistema.

Bombas lógicas

Las bombas lógicas son partes de código de ciertos programas que permanecen sin realizar ninguna función hasta que son activadas; en ese punto, la función que realizan no es la original del programa, sino que generalmente se trata de una acción perjudicial.

Los activadores más comunes de estas bombas lógicas pueden ser la ausencia o presencia de ciertos ficheros, la ejecución bajo un determinado UID o la llegada de una fecha concreta; cuando la bomba se activa va a poder realizar cualquier tarea que pueda realizar la persona que ejecuta el programa: si las activa el root, o el programa que contiene la bomba está setuidado a su nombre, los efectos obviamente pueden ser fatales.

Virus

Los efectos de los virus son ampliamente conocidos en algunos sistemas operativos. Entre ellos se nombran algunos.

Gusanos

Un gusano es un programa capaz de ejecutarse y propagarse por sí mismo a través de redes, en ocasiones portando virus o aprovechando bugs de los sistemas a los que conecta para dañarlos. Al ser difíciles de programar su número no es muy elevado, pero el daño que pueden causar es muy grande.

Caballos de Troya

Los troyanos o caballos de Troya son instrucciones escondidas en un programa de forma que éste parezca realizar las tareas que un usuario espera de él, pero que realmente ejecute funciones ocultas

Programas conejo o bacterias

Bajo este nombre se conoce a los programas que no hacen nada útil, sino que simplemente se dedican a reproducirse hasta que el número de copias acaba con los recursos del sistema (memoria, procesador, disco...), produciendo una negación de servicio.

Cuanta Seguridad se requiere?

"Los datos deben protegerse sólo hasta que pierdan su valor".(Mario Farías-Elinos.2002)
Se habla, por tanto, de la caducidad del sistema de protección: tiempo en el que debe mantenerse la confidencialidad o secreto del dato.
. "Las medidas de control se implementan para ser utilizadas de forma efectiva. Deben ser eficientes, fáciles de usar y apropiadas al medio".
– Que funcionen en el momento oportuno.
– Que lo hagan optimizando los recursos del sistema.
– Que pasen desapercibidas para el usuario.
Ningún sistema de control resulta efectivo hasta que es utilizado al surgir la necesidad de aplicarlo.

Biometría.

Los sistemas biométricos de seguridad están basados en documentos, archivos de información relacionada a la identificación de las personas, estableciendo los patrones necesarios para el desarrollo de esta tecnología. Estos métodos biométricos ya son utilizados en varios ámbitos y principalmente con el propósito de reemplazar a los ya existentes como passwords, tarjetas de crédito, consultas bancarias en cajeros automáticos.
La biometría toma en cuenta elementos morfológicos únicos y propios de cada persona.

Sus inicios.

La utilidad de la huella digital surgió cuando al científico Henry Faulds, que se encontraba en Japón en 1880, se le ocurrió tomar muestras dactilares de las personas que habitaban el poblado para compararlas con otras huellas obtenidas en excavaciones arqueológicas y determinar su antigüedad. Durante esta labor se percató de que, independientemente de su raza, las huellas eran diferentes en cada persona. Cuentan que algunos pobladores le robaron ciertas pertenencias y gracias al banco de huellas que tenía en su poder pudo descubrir a los ladrones.

El nacimiento de las técnicas de identificación a través de las huellas dactilares, a pesar de transcurrido el tiempo es la herramienta más eficaz para la identificación de personas. Junto a esta forma de identificación han surgido el ADN y el iris en el ojo, por ejemplo, cómo otras formas adicionales para corroborar las identidades y ya no son parte de la fantasía cómo lo vimos en las películas de acción sino son los llamados métodos biométricos de identificación.

Reconocimiento biométrico

La interactividad y lo digital del mundo ha obligado a cambiar las formas de vida, tal es el caso que cuando se quiere chequear un saldo de una cuenta bancaria se acude a Internet y entrando con un usuario permitido y unas claves se puede ver el estado de cuenta, al parecer el diario vivir se han reducido a números o claves secretas con las que las personas son identificadas, ya ocurre así cuando por ejemplo se acude una biblioteca y se quiere retirar un libro se debe recordar el número de identificación y si no lo sabe la persona, pues tan sencillo que no existe para los efectos y no pueden prestar el servicio. Aunque esto le ha cambiado la sensibilidad al asunto para el gusto de muchos, es más eficiente y rápido.

Para que todas estas operaciones funcionen a la perfección se necesitan algunas herramientas adicionales como la encriptación, el cifrado, la firma digital, las cuales permiten obtener la certeza necesaria para continuar a bordo de este mundo digital.

La forma en que el mundo ha ido informatizándose ha sido a través de los sistemas de seguridad donde la prioridad de los sectores industriales en el mundo han ido cambiando de tal forma que la eficiencia y la efectividad ha sido enfocada en la medida que cuentan con un buen sistema de cómputo para prestar un buen servicio, así es cómo los sistemas de seguridad han ido evolucionando de lo digital a lo *biométrico.*

Para proteger la privacidad de las personas ha sido necesario idear toda una nueva infraestructura que, aunque ha costado millones de dólares, en estos momentos se encuentra desarrollando tecnologías basadas en la biometría como pueden ser los patrones de las huellas digitales, del iris, del tono de voz.

Los sistemas biométricos de seguridad están basados en documentos, archivos de información relacionada a la identificación de las personas, estableciendo los patrones necesarios para el desarrollo de esta tecnología. Estos métodos biométricos ya son utilizados en varios ámbitos y principalmente con el propósito de reemplazar a los ya existentes como passwords, tarjetas de crédito, consultas bancarias en cajeros automáticos.

La biometría toma en cuenta elementos morfológicos únicos y propios de cada persona.

Identificación biométrica

Tal y cómo aparecen las investigaciones criminales donde las huellas digitales muchas veces llevan a identificar al responsable del delito y al igual que sucede cuando nacen las personas y son registradas con nuestra huella digital, la identificación biométrica se utiliza en las personas.

La utilización de estos métodos biométricos han llevado a las industrias a crear software y hardware, basando sus sistemas de seguridad a la extracción de puntos característicos de la huella digital, con este proceso la información dactilar se ha reducido a un algoritmo matemático, que se verá con detalle más adelante.

En la actualidad, algunos organismos gubernamentales y empresas de alta seguridad han desarrollado sistemas de acceso a espacios físicos con identificaciones biométricas utilizando técnicas de Identificación Automática de huellas dactilares, para regular el acceso a espacios físicos o información restringida.

Uno de los beneficios de utilizar los métodos biométricos de identificación es que los elementos mismos de identificación y la información contra cual se confrontan los datos es intransferible.

Otra técnica de autenticación utiliza el reconocimiento facial, por medio del los caracteres almacenados en las bases de datos relacionados al programa de reconocimiento, verificarán las características y en cuestión de segundos aceptará o rechazará la solicitud.

La forma de reconocimiento biométrico basado en la voz, con ciertos caracteres prefijados y con ciertas palabras claves complementan el método para tener acceso y de esta manera la voz del usuario es comparada con un registro anterior del sistema.

El patrón de reconocimiento a través del iris conforma el método más avanzado de identificación de personas, así como las demás formas, los métodos biométricos tienen el 98% de efectividad.

Tipos de biometría.

Puede decirse que la Biometría (o mejor dicho, Identificación Biométrica), es la técnica por la que se pretende identificar a una persona a partir de sus rasgos físicos y/o de comportamiento. Esta identificación se puede hacer por medios manuales o por medios automáticos.

Es preciso aclarar que, aunque muchos investigadores y empresas llevan trabajando décadas en esta tecnología, no ha sido sino hasta hace unos tres años cuando la Biometría ha sufrido un gran auge, en cuanto al interés de empresas y administraciones por su uso. El motivo tiene sus orígenes en los acontecimientos ocurridos en septiembre de 2001 en EE.UU., y en el hecho de que, a raíz de ello, el gobierno americano y las asociaciones de aviación consideraran la Biometría como "la solución a la falta de seguridad". Si bien su uso puede incrementar la seguridad de un sistema, un sistema no se puede considerar seguro por el simple hecho de utilizar Biometría. Los tres objetivos fundamentales que persigue la Biometría son: (Tecnologías Biométricas Aplicadas a la Seguridad, 2002)

• Realizar la identificación positiva de una persona, en aquellos entornos donde no se puede contar con un agente que lo realice (por ejemplo en todos y cada uno de los cajeros automáticos)

• Ayudar a un agente a realizar la verificación de un individuo, evitando así errores por cansancio humano.

• Proporcionar al usuario un modo más "humano" de interactuar con el sistema, evitando así el rechazo por parte de algunos colectivos de usuarios, así como los riesgos de pérdida u olvido.

Estos objetivos, especialmente el tercero, una vez cumplidos pueden redundar en un incremento de la seguridad del sistema, aunque sea a partir de la eliminación de puntos débiles del sistema actual.

Estructura de un Sistema de Identificación Biométrica

Independientemente de si el sistema se diseña como un sistema de Reconocimiento o de Autenticación, y de forma independiente a la técnica biométrica utilizada (huella, iris,rostro, etc.), a la hora de desarrollar un sistema de identificación biométrica, se mantiene un esquema común. Dicho esquema se basa en dos fases totalmente diferenciadas.

1. Reclutamiento: En esta fase, se toma una serie de muestras del usuario, y se procesan, para posteriormente extraer un patrón, el cual se almacenará y será el conjunto de datos que caracterizará a ese usuario. Si se captura más de una muestra, el patrón suele ser el resultado de una media de las características obtenidas. Este proceso se hace de forma supervisada, es decir, existe una persona encargada de controlar cómo se produce la captura de los datos, así como de asegurar la identidad de la persona que se está reclutando en el sistema. Esta fase se realiza una única vez (es posible que a lo largo de la vida, por motivos de gestión de incidencias haya que repetirlo alguna otra vez). Es más que recomendable que, durante la realización de esta fase, se aproveche para formar al usuario en el uso del sistema, y a aclararle todas las dudas que pudiera tener.

2. Utilización: Una vez que se tiene almacenado el patrón del usuario, éste puede utilizar el sistema con normalidad, permitiendo que se le tomen sus muestras y que sus características se comparen con el patrón almacenado, determinando el éxito o fracaso de esa comparación.

Técnicas biométricas más importantes

Cualquier parámetro del cuerpo humano y de su comportamiento puede ser utilizado como punto de entrada a un sistema de identificación biométrica, siempre que se sea capaz de extraer características únicas del individuo de dicho parámetro. Esto hace que exista una gran variedad de técnicas biométricas en las que es preciso considerar los siguientes criterios:(Tapiador y Sigüenza, 2002).

- *Universalidad*: Si las características se pueden extraer de cualquier usuario o no, o el porcentaje de usuarios que pueden utilizar dicha técnica.
- *Unicidad:* Probabilidad de que no existan dos sujetos con las mismas características.
- *Estabilidad:* Si las características que se extraen permanecen inalterables con relación a diversos parámetros (tiempo, edad, enfermedades...).
- *Facilidad de captura:* Si existen mecanismos sencillos de captura de los datos.
- *Rendimiento:* O tasas de acierto y error.
- *Aceptación por los usuarios*.
- *Robustez frente a la burla del sistema:* Si la técnica puede reconocer el falseamiento de los datos capturados (uso de fotos, dedos de latex, etc.).
- *Costo*.

Atendiendo a estos parámetros y a las técnicas existentes, no se puede afirmar que una técnica sea la mejor de todas; dependerá de la situación y el entorno. Por ejemplo, una puede ser la que mayor rendimiento, unicidad, universalidad y estabilidad dé, pero puede ser excesivamente cara, y que su implantación sea inviable, así como si es rechazada por los usuarios.

Sistemas Biométricos Aplicados.

Entre estos sistemas los más reconocidos se tienen:

Reconocimiento de Huellas dactilares

La identificación única por medio de las huellas dactilares o ha estado presente durante muchas décadas. Quizás por eso, las aplicaciones biométricas en computación tienen también su tiempo; fue a principios de los 80 en que aparecieron los primeros sistemas de este tipo.***(Ormella y Gómez 2002)***

De hecho el sistema parte de un proceso similar al conocido; se trata de tomar las huellas dactilares. El escaneado o lectura electrónica se convierte a un código digital que se compara con los existentes en la base de datos. Pese a la gran exactitud de este método, las lecturas pueden complicarse por suciedad, grasa, quemaduras, lastimaduras, cicatrices, etc. que deformen la imagen como para verse representada de manera lo suficientemente diferente de la original y provocar un rechazo equivocado.

Entre los usos de este sistema se pueden mencionar el acceso a aplicaciones financieras, para autorización de transacciones de valor elevado en bancos, acceso a redes, estaciones de trabajo y recursos de red, verificaciones del horario de trabajo, y hasta registro de votación.

La operación de un sistema de este tipo puede incluir el escaneado de los dedos desde diferentes ángulos para tener una información más completa.

La información en sí misma consiste en establecer dos componentes: patrón y pequeños detalles.

El patrón se refiere a las líneas y surcos o espacio entre líneas que conforman la huella dactilar, Los patrones básicos son tres: lazo, arco y espiral.

En un patrón tipo lazo, las líneas comienzan de un lado del dedo, llegan hasta un tope aproximadamente en el centro de la yema del dedo y regresan hacia el mismo lado.

Se tiene un patrón en forma de arco cuando las líneas comienzan al costado del dedo y llegan al centro de la yema y siguen hacia el otro lado del dedo, formando precisamente un arco que pasa por la zona central de la yema.

Finalmente, en un patrón en forma de espiral las líneas forman círculos aproximadamente concéntricos al centro de la yema.

En muchos casos, las huellas dactilares muestran una combinación de estos patrones.

Referente a los pequeños detalles de los puntos singulares se mencionan los siguientes términos:

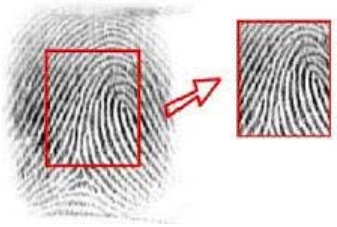
• Bifurcación: El punto donde una línea se divide en varias líneas llamadas ramas.

• Divergencia: El punto donde se separan varias líneas prácticamente paralelas.

• Cercado: Punto en que una línea que se divide en dos ramas que más adelante se vuelven a juntar.

• Terminación: Donde termina una línea.

Cada uno de los detalles mencionados se posiciona en un sistema de ejes coordenados x,y registrándose, entre otras características, la curvatura de las líneas y el espacio entre las mismas en el punto singular**.** *Cómo se muestra en la figura a la izquierda.*



Los sistemas de identificación o de reconocimiento de uno entre muchos, son conocidos como AFIS (Sistemas de Identificación Automática de huellas dactilares.)

A su vez hay dos tipos de aplicaciones AFIS: forense y civil. En el primer caso se capturan múltiples imágenes de cada dedo desde diferentes ángulos. Las aplicaciones civiles, en cambio, trabajan generalmente con una única imagen plana de algunos dedos solamente.

Por su parte, los sistemas de verificación, también trabajan con imágenes planas pero de un único dedo, haciendo en pocos segundos el reconocimiento de uno contra uno.

Reconocimiento de Rostros

En este sistema, no es una tarea fácil reconocer adecuadamente las formas y posicionamiento de características distintivas de un rostro. Este es uno de los motivos de que este mecanismo sea de desarrollo más reciente.

Este método tiene la ventaja que no obstruye al usuario y hasta puede registrar directamente una foto del usuario. Para realizar este registro, a veces se requieren cámaras costosas (aunque en otros casos basta una simple cámara) y aún así el sistema no es totalmente seguro especialmente a nivel de aceptaciones equivocadas. Por otra parte los rostros cambian con el tiempo, por tanto se requieren actualizaciones periódicas.

Los productos de este tipo trabajan con varias imágenes de cada usuario y el proceso de reconocimiento está regido por una serie de reglas que conducen a una identificación efectiva. Tanto es así que algunos usan tecnología de redes neuronales propias de un esquema de inteligencia artificial que básicamente adquieren conocimiento de la experiencia. La cámara puede estar en algunos casos a un metro o un poco más de distancia. En general la captación es en movimiento para que no se pueda usar una foto tratando de engañar al sistema. En otros casos se trabaja con vistas de frente y de perfil.

En la imagen capturada analiza la geometría de la cara con parámetros tales como la distancia entre los ojos y la nariz, curvatura de los huesos, asimetrías de puntos notables, etc. Estos sistemas están diseñados para considerar el efecto de barbas, lentes o anteojos, y sombreros.

Si bien el sistema es muy exacto, su uso principal se orienta a la verificación de una persona determinada y no precisamente a la identificación de una entre muchas.

Los sistemas de reconocimiento de rostros se usan en aplicaciones cómo operaciones financieras en general incluyendo e-commerce, atención de salud de sistemas de seguridad social, control de fronteras (junto con reconocimiento de la voz, y seguridad en general.).

La primera etapa consiste en la detección de la imagen capturada de la cual se separan los elementos faciales eliminando información extraña (como la barba y anteojos ya mencionados). El software analiza la imagen buscando determinar las estructuras típicas de los elementos más importantes (como ojos y nariz) con las que calcula la cara completa recortando el fondo original y ubicándola dentro de un recuadro rectangular llamado ***máscara binaria. .(Ormella y Gómez, 2002)***

La segunda etapa es la del reconocimiento o comparación de la imagen resultante con las de la base de datos.

El resultado es entonces que una cara resulta ser la combinación de dichas áreas únicas de esa cara.

Algunos productos trabajan con imágenes térmicas logradas con cámaras infrarrojas que permiten crear mapas de venas subcutáneas. Estos sistemas resultan más precisos especialmente al no depender de cambios en la superficie de la piel y, por supuesto, pueden llegar a operar en la oscuridad.

La fase final del reconocimiento comparará las características únicas encontradas con las características correspondientes de la base de datos.

Geometría de las manos y dedos

En una operación que demora poco más de un segundo, un sistema de este tipo permite obtener un registro tridimensional de las principales características de la mano y/o los dedos tales como longitud, ancho y altura, algunas áreas particulares, etc. así como posiciones relativas de dedos, nudillos, etc.

Con esa información, el sistema crea un mapa tridimensional del contorno de la mano. En la práctica, sin embargo y con los productos actuales, no se alcanza el nivel de eficiencia logrado con otros sistemas biométricos. Además, el análisis puede verse afectado por heridas, desgarros e hinchazones.

Uno de los primeros usos del mecanismo de geometría de manos fue en el sistema de seguridad de los juegos Olímpicos de 1996. De hecho el bajo costo y facilidad de uso de estos sistemas está facilitando su difusión en aplicaciones muy diferentes. Se lo está usando, por ejemplo, para identificación personal en operaciones con cajeros automáticos y tarjetas de crédito.

Y mientras en combinación con PIN algunas grandes compañías realizan el control de asistencia del personal, se encuentran también en centros de datos así como para el acceso a laboratorios o centros de seguridad.

Los sistemas de geometría de extremidades superiores responden a tres variantes diferentes con su propia tecnología especialmente de hardware: geometría de las manos, de un dedo y de dos dedos.

El primer sistema trabaja colocando la mano sobre una placa que tiene guías para ubicar cada uno de los dedos. La cámara toma una fotografía estableciendo hasta casi un centenar de características diferentes.

Para los sistemas de geometría de dedos el dispositivo de captura tiene un pequeño pistón donde se ubica el dedo. El sistema tiene en su parte interna un conjunto de pequeñas ruedas que ruedan alrededor del dedo cuando éste empuja el pistón. De esta manera se levantan mediciones de doce secciones diferentes a lo largo de unos cuatro centímetros del dedo.

Finalmente, el sistema de dos dedos trabaja con el dedo índice y el del medio.

En esta categoría también es usual incluir el reconocimiento de la palma de la mano por medio del escaneado correspondiente que se analiza luego de manera similar al reconocimiento de huellas dactilares ya comentado.

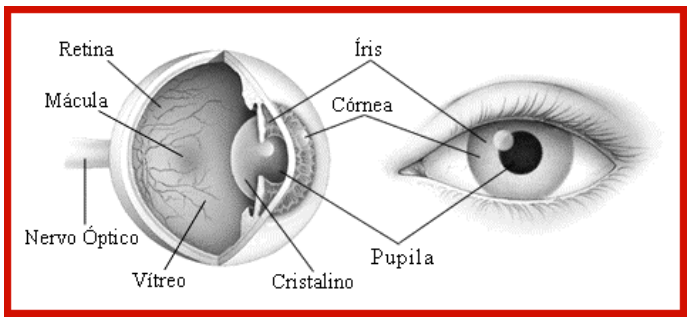
Reconocimiento de Iris y Retina.

Los sistemas basados en los ojos de las personas generalmente son los que ofrecen mayor seguridad entre los métodos biométricos, gracias a la unicidad de los patrones individuales y la calidad de los dispositivos de captura. Se usa una cámara de video para capturar o los patrones de los tejidos del iris o las venas de la retina.

Reconocimiento del Iris

El iris es la franja de tejido que rodea la pupila del ojo. Tiene una estructura compleja de estrías, anillos, surcos, coronas y flecos que ofrece prácticamente infinitas variaciones incluso entre ambos ojos de la misma persona; y que además, permanece constante con el tiempo.

Los datos capturados se procesan por medio de complejos algoritmos matemáticos.



Las implementaciones de este sistema responden a dos tipos: activo y pasivo.

Los productos del tipo activo requieren que el mismo usuario quede en foco con la cámara, moviéndose hacia atrás y adelante entre unos 15 a 30 cm. La otra posibilidad, de caracter pasivo, consiste en un juego de cámaras que ubican automáticamente la cara y ojos de los usuarios. Obviamente que este sistema es más costoso que el activo.

Como para la operación se necesita ubicarse a poca distancia de la cámara, se aprecia cierto rechazo en las personas.

Escaneado de Retina

La retina es la capa más interna, llena de vénulas o venillas de la pared posterior del globo ocular. La retina también permanece bastante estable con el tiempo salvo cuando resulta afectada por algunas enfermedades.

Con una imagen adecuada se puede establecer un mapa muy preciso y único del patrón de conductos venosos.

Con este sistema se hace que un rayo de luz incandescente incida sobre la retina para retornar al escáner de captura. Para un resultado adecuado la imagen debe estar bien enfocada y mantenerse quieto el usuario, lo que agrega más complejidad además del temor, y consiguiente rechazo, que puede causar el haz de luz sobre el ojo.

Autenticación de la Voz

Si bien este sistema es menos seguro que el de las huellas dactilares y el escaneado de iris o retina, su costo lo hace más accesible.

Su principal uso se encuentra en aplicaciones de seguridad en el acceso telefónico, para verificación de acceso a correo de voz, activación de tarjetas de crédito y hasta para constatar la identidad de personas en libertad condicional con reclusión domiciliaria.

En la voz que se registra se analizan principalmente el tono (intensidad o fuerza) y la altura (frecuencia) de los sonidos, generalmente por medio del análisis eléctrico de la densidad de la energía y formas de onda (por componentes armónicos), así como las inflexiones o cadencia en el hablar y el propio comportamiento lingüístico.

Para el registro inicial generalmente se repite varias veces una misma frase y/o una serie de frases. De esta manera se establece el patrón individual contra el cual se compara cada vez que se recurra al sistema para verificación del usuario.

La exactitud del sistema puede verse afectada principalmente por el ruido de fondo y las características del elemento que capta el sonido (teléfono o un micrófono), así como por variaciones naturales como cambios de humor, fatiga, transcurso del tiempo, etc.

Reconocimiento de Firma

No se refiere a la firma digital. La verificación tradicional de firmas es ampliamente conocida especialmente en el medio bancario. El sistema biométrico correspondiente, por su parte, goza precisamente de una aceptación similar en este caso como medio de verificación.

Este sistema ha encontrado uso en empresas de seguro y hospitales así como en general para autenticar documentos electrónicos.

Sin embargo, ahora no se trata de observar manualmente con mayor o menor precisión la forma de una firma en comparación con la imagen de una firma registrada anteriormente. Un sistema de Verificación de Firmas establece y mide características de la

firma, especialmente las relacionadas con el modo como se firma. Para ello suelen usarse lapiceros o *stylus* especiales sobre tabletas gráficas digitalizadoras o simples *palmtops*. Algunas de las características analizadas son la presión que se ejerce sobre el lapicero en las diferentes partes, puntos en que el lapicero se separa del papel, orden, velocidad y aceleración de los trazos, y agudeza de los lazos.

Para medir características como la aceleración se necesita identificar los trazos en planos de ejes coordenados con una resolución de fracción de milímetro que se muestrean periódica y sincrónicamente. La representación matemática de todas las características se guarda adecuadamente codificada para ser tomada como base cada vez que se recurra al sistema. Algunas limitaciones de este sistema se refieren a que los cambios naturales que se producen en las firmas con el tiempo, pueden aumentar el nivel de rechazos equivocados, a lo que se suma el mayor costo respecto de otras soluciones.

En algunos casos se trata de incorporar la firma a un documento usando para el caso una suerte de *token* biométrico de aquella incorporado al propio documento, de modo tal que la firma se invalida si se altera el documento. Generalmente el sistema capta hora, fecha, identificación de la PC, información de chequeo del contenido del documento y alguna otra información procurando acotar el evento en sí de la firma. Sin embargo esto no demuestra que la firma realmente es auténtica. Lo mencionado en este párrafo simplemente señala un grupo de productos que procuran incorporar la firma a un documento para dar a éste validez respecto de su autor. Son formas más simples pero no seguras de suplir las conocidas firmas digitales ya mencionadas.

Adicionalmente, si las necesidades de seguridad imponen ciertas exigencias mayores se puede combinar el uso de algunas de las soluciones biométricas junto con tarjetas inteligentes.

Algunos ejempos de Biometría aplicados.

Se puede citar varios ejemplos reales que demuestran que la tecnología biométrica es una realidad que se está implementando con éxito en muchos ámbitos de la industria.

En el aeropuerto de Schiphol se utiliza desde el mes de Noviembre del 2001 un sistema de reconocimiento del iris para incrementar la seguridad y agilizar el sistema de gestión de los pasajeros de vuelos frecuentes. El sistema se basa en una tarjeta inteligente que contiene

encriptado el patrón del iris del individuo. Este patrón se compara con la lectura del iris que se obtiene cuando el pasajero pasa por el control biométrico; si existe una correlación positiva entre el patrón almacenado en la tarjeta y el obtenido de la lectura entonces la verificación es positiva. Este sistema también se está utilizando en el aeropuerto de Hearthrow de Londres y en el aeropuerto de Miami (*Claret,* **2003**).

Otro ejemplo es el del Deutsche Bank en Frankfurt que desde hace tiempo utiliza biometría de reconocimiento de la huella digital para proteger el acceso a las salas de servidores. En el ámbito nacional, recientemente leíamos una noticia sobre el nuevo sistema de control de la inmigración basado en el reconocimiento de la huella dactilar que se está utilizando en Melilla.Sin embargo, la tecnología biométrica aún no ha despegado y la mayoría de los ejemplos se encuentran en el entorno del control de la criminalidad y de las altas finanzas, como demuestran los ejemplos anteriores. Existen muchas tecnologías biométricas y no todas son lo que sus fabricantes predican. La biometría es un mercado enorme y se ha de analizar muy bien cada producto para estar seguro de que puede cumplir las expectativas demandadas por el cliente.

Pruebas de Violación a tecnología Biométrica.

Se ha de saber por la experiencia que nada es infalible y como toda tecnología o sistema de seguridad puede tener su punto débil, es el caso realizado por un criptógrafo japones , estudiante de Tsutomu Matsumoto, estudiante de informática en la Universidad Nacional de Yokohama. El experto hizo la prueba capturando las huellas depositadas en un vaso. Primero las realzó con adhesivo, después las fotografió con una cámara digital, mejorando, mediante un programa de retoque, el contraste de la imagen e imprimiendo a continuación el resultado en una hoja transparente. Utilizó esta transparencia para grabar la huella en cobre y de ahí la pasó a un falso dedo de gelatina, con una textura similar a la que muestran los ositos de goma y otros dulces.(IBLNEWS, 2002)

El japonés burló los detectores en el 80 % de los casos, poniendo así en jaque esta tecnología biométrica, en cuyo desarrollo pesan grandes intereses económicos. Conocido el descubrimiento, que fue presentado el martes 21/06/2002, en Seúl (Corea del Sur), algunos expertos opinaron que "los resultados son suficientes para enviar a los fabricantes de sensores a laboratorio del comienzo". La técnica empleada por el criptógrafo japonés, funciona con 11 diferentes lectores de huellas dactilares**.**

Futuro de la biometría.

Estos sistemas de biometría son soluciones de alta tecnología que responden a las nuevas exigencias en seguridad del mundo cambiante. Así que en un futuro bien cercano las personas podrán estar accesando su respectiva cuenta de banco o abordando un avión utilizando sus propios ojos o sus huellas digitales – identificadores que nunca podrá olvidar en su casa - utilizando así una de las tecnologías más avanzadas en seguridad disponibles. Se cree en la biometría como método de autenticación, sin embargo se están estudiando con métodos más precisos y rápidos e inteligentes como la lectura y reconocimiento de ADN.

Conclusiones y recomendaciones.

Viendo los sistemas juntos se mencionan las ventajas y desventajas más concretas que caracterizan a las diferentes soluciones como se muestra en la siguiente tabla.

Tabla número 1.

Comparación entre características Biometricas analizadas.

Biometría	Ventajas	Desventajas
Huellas dactilares:	Seguro y disponible especialmente para identificación. No acepta ni aún una cinta donde se haya levantado una impresión no visible a partir de una huella espolvoreada.	Resistencia al uso por connotaciones criminales.
Reconocimiento de Rostros:	Apto para aplicaciones de identificación de uno contra muchos.	Costoso y sujeto a engaños con fotos montadas sobre narices semejantes.
Geometría de las manos:	Fácil de usar.	Sujeta a cambios físicos, no muy adecuada para grandes bases de datos de sistemas de identificación y verificación.
Escaneado de iris:	Muy seguro para aplicaciones de identificación de uno contra muchos.	Costoso, sensible a los movimientos del usuario y ocupa mucho espacio.
Escaneado de Retina:	Muy seguro para aplicaciones de identificación.	Costoso, no puede usarse con algunos usuarios por su sensibilidad a un escaneado infrarrojo o láser en los ojos.
Análisis de la voz:	Para aplicaciones de verificación local o remota siendo de bajo costo.	Sujeto a cambios físicos y cierta facilidad de engaño con voces semejantes incluso con grabaciones en algunos casos
Verificación de Firma:	Alto nivel de aceptación para verificación de un usuario determinado.	Sujeta a cambios físicos.

Fuente recopilada por el autor.

Se puede decir que los productos en general pueden hacerse más seguros si se los vuelve más "celosos" en sus comparaciones con el perfil almacenado. Pero al mismo tiempo que se gana bajando la tasa o porcentaje de aceptaciones equivocadas, también subirá la tasa de rechazos equivocados. Además, un aumento de la sensibilidad del sistema acarrea mayor procesamiento y retardo en el reconocimiento.

Entonces hay que plantearse hasta qué punto se puede aceptar una cierta cantidad de rechazos equivocados con las consiguientes molestias para los usuarios y administradores, con tal de asegurar un mayor grado de seguridad al reducir consecuentemente la tasa de aceptaciones equivocadas.

Tanto en verificación como en identificación, si la comparación es exitosa el sistema biométrico le concede a la persona ciertos privilegios como, por ejemplo, acceso a su cuenta de banco o permiso para abordar un avión. Cuando la comparación es fallida, los privilegios son negados.

Sin embargo con el fin de reforzar una determinada seguridad, ya que habrá formas en las que violen o burlen los sistemas valiéndose de cualquier artimaña, se considera hacer una combinación de estos sistemas biométricos, que una vez establecidos las probabilidades de violar la seguridad son menos.

Una de las preocupaciones más relevante en el uso de sistemas biométricos es la posibilidad de violaciones a la privacidad personal. Por privacidad personal se entiende como la habilidad que tiene el individuo para controlar información sobre sí mismo, es decir, el conocimiento que tiene la persona de a quién, cuándo y con qué propósito se utiliza su información personal. Así que su manejo inapropiado puede causar preocupaciones serias.

Bibliografía.

Bruno, Mark. BIOMETRICS' DAY HAS COME**.** Banker; Dec2001, Vol. 111 Issue 12, p56, 3p, 1 graph, 3bw. Article

Calderon, Thomas G.1.Towar a biometric security Layer in Accounting Systems. Journal of Information Systems; Fall2003, Vol. 17 Issue 2, p51,20p, 2 charts, 4 diagrams. Article .Número de acceso: 12056799

Carlos Ormella Meyer e Ing. Hernán Gómez Acosta | Junio 2002 |. Autenticación biométrica .Articulo de la edición 81 (Diciembre de 1999) de la revista LAN & WAN que trata en profundidad los distintos tipos de reconocimiento biométrico. Artículo.

D. Valentino Cornejo López. Detrás de la Huella.Universidad Panamericana desde 1996, encargado de sistemas de información y nuevas tecnologías en la Biblioteca. Desde el año 2000 lleva a cabo labores de investigación en el Instituto de Investigaciones Sociales y de Opinión Pública A.C.Artiículo . Informática Profesional. Año 17 | Nº 85 | Enero de 2003.

Fratto, Mike.Are Biometrics The Answer?.Network Computing; 2/20/2003, Vol. 14 Issue 3, p72, 2p, 1c.Article.

Fisher, Dennis, eWeek. La BIOMETRIA ENCIERRA EN LA EMPRESA.15306283, 03/26/2001, Vol. 18, Fascículo 12.Base de datos: Business Source Elite
Sección: Las noticias & el Análisis La BIOMETRIA ENCIERRA EN LA EMPRESA.

Gerardo Torrez.Titulo : Deja Huella. PC Magazines Vol. .16 / No 04 Pág. 7,8. Abril 2005.

Grimes, Brad. PC Magazine.Biometric La seguridad, (4/22/2003) Vol. 22, Fascículo 7 Base de datos**:** *Business Source Elite.*

Marino Tapiador y Juan A. Sigüenza.Tecnologías Biométricas Aplicadas a la Seguridad (ISBN: 8478976361 Acceso a Internet 06/06/2005.

Mario Farías-Elinos .Seguridad en los Sistemas de Cómputo.Coord. del grupo de Seguridad en Internet-2. Laboratorio de Investigación y Desarrollo de Tecnología Avanzada (LIDETEA)Universidad La Salle.
http://www.ci.ulsa.mx/lidetea
http://seguridad.internet2.ulsa.mx/

Moss, Brenda. GETTING PERSONAL.Base de datos: Business Source Elite. Health Facilities Management; Sep2002, Vol. 15 Issue 9, p20, 5p. Article . Número de acceso: 7437082.

Mireia Claret | Mayo 2003.Seguridad biométrica: El éxito de una tecnología que ya es una realidad .
http://www.rediris.es/cert

Nelson, Matthew G.Pentagon Enlists IT in Face-Off With Terrorists. InformationWeek.8/6/2001 Issue 849, p12, 1/4p. Article
UNITED States. -- Defense Advanced Research Projects Agency Empresa/Entidad: VISIONICS Corp. DUNS Number: 147586762.

Villalón, Huerta Antonio. Seguridad en Uníx y Redes. Ver 2.1 Julio 2002
http://www.rediris.es/cert/doc/unixsec/unixsec.pdf
http://iblnews.com/news/noticia.php3?id=36583
accseso 17/06/2005.

Taschek, John. AN EYE ON BIOMETRICS. eWeek; 11/19/2001, Vol. 18 Issue 45, p51, 2p, 2c . Article .Número de acceso: 5567372.