

Introducción a los Biométricos

Después de los lamentables atentados del 11 de septiembre de 2001, se ha creado una enorme demanda de productos de seguridad. Por su alto nivel de seguridad, los productos biométricos han acaparado gran parte de la demanda. Aunque en nuestro continente son productos considerados innovadores, existen desde hace más de 15 años y han sido principalmente utilizados en Europa e Israel, donde se presentaba la mayor cantidad de secuestros y atentados terroristas durante los años 70s y 80s.

¿Qué es la biometría informática?

Pero, ¿qué es la biometría? Vale aclarar que la palabra biometría tiene dos significados. El concepto tradicional de biometría se refiere a la aplicación de las técnicas matemáticas y estadísticas al análisis de datos en las ciencias biológicas. Esta definición enmarca una disciplina que se inició a principios del siglo XX.

El contexto tecnológico de la palabra biometría se refiere a la aplicación automatizada de técnicas biométricas a la certificación, autenticación e identificación de personas en sistemas de seguridad. Las técnicas biométricas se utilizan para medir características corporales o de comportamiento de las personas con el objeto de establecer una identidad. Para diferenciar estos conceptos, organizaciones y autores han dado un nombre compuesto al contexto tecnológico como biometría informática y autenticación biométrica. En adelante, en este documento haremos referencia de la palabra biometría enmarcada al contexto tecnológico.

La biometría busca la automatización de tareas que involucran el reconocimiento del individuo. Las máquinas no evalúan ningún otro factor al tomar una decisión, sólo se evalúa la identidad. Esto resta cualquier factor subjetivo que pueda comprometer la seguridad.

Seguridad y productos biométricos

Los sistemas de seguridad utilizan tres métodos de autenticación:

- o Algo que usted sabe: una contraseña, un número de identificación (PIN), etc.
- o Algo que usted tiene: una llave, tarjeta de proximidad, smart card, etc.
- o Quién es usted: seguridad biométrica.

De los tres métodos, la biométrica es la más segura y conveniente. Una contraseña puede ser traspasada, una llave puede ser robada, pero la identidad no.

Tipos de productos biométricos

Aunque las técnicas biométricas usan una combinación de factores corporales y de comportamiento (por ejemplo la medición de la biometría basada en huella digital variará de acuerdo a la manera en que se coloca el dedo), la clasificación de las técnicas biométricas facilita su estudio. La medición de las características corporales de las personas es conocida como biometría estática. Los principales estudios y aplicaciones de la biometría estática están basados en la medición de huellas digitales, geometría de la mano, iris, forma de la cara, retina y venas del dorso de la mano. Existen también, pero menos usadas, las técnicas biométricas basadas en forma de las orejas, temperatura corporal (termografía) y forma del cuerpo.

La medición de las características de comportamiento de las personas es conocida como biometría dinámica. Los principales estudios y aplicaciones de la biometría dinámica están basados en el patrón de voz, firma manuscrita, dinámica del tecleo, cadencia del paso y análisis gestual.

Cómo funcionan los productos biométricos

Para realizar la autenticación biométrica, primero se debe registrar a los individuos que van a hacer uso del sistema. Para el registro (en inglés, enrollment) se utiliza un dispositivo biométrico para examinar el atributo físico o de comportamiento elegido. Un software o firmware se encarga de cuantificar los datos examinados y transformarlos en datos matemáticos. El conjunto de estos datos matemáticos constituye la plantilla (en inglés, template) que identifica al individuo. La plantilla y un dato asociado al individuo (como por ejemplo el nombre o un PIN) son guardados electrónicamente. La lectura del atributo no se cuantifica en su totalidad, de esta manera no es posible reproducir a partir de la plantilla un miembro falso o un comportamiento artificial.

La autenticación posterior se realiza cuando el individuo presenta su rasgo corporal o muestra su comportamiento ante un dispositivo biométrico. Nuevamente se cuantifica los datos del rasgo en una nueva plantilla para compararlos contra la plantilla guardado. La búsqueda de la plantilla guardada puede realizarse de dos maneras. La primera es una búsqueda uno a muchos (1:N), solamente se presenta el rasgo y el sistema se encarga de buscar entre todas las plantillas guardadas, quién es el individuo, esto es conocido como identificación. Este método requiere un mayor tiempo de búsqueda y es utilizado en bases de datos pequeñas o en aplicaciones criminalísticas.

El segundo método es una búsqueda uno a uno (1:1), donde el individuo presenta adicionalmente su nombre o número de identificación. El sistema se encarga de buscar la plantilla guardada que esté bajo el nombre o número de identificación solamente, y realiza la comparación. Esto es conocido como verificación, y es utilizado en la mayoría de las aplicaciones biométricas.

Para que se certifique al individuo, la comparación no necesariamente resulta en una igualdad entre ambas plantillas. En realidad, pueden pasar años antes de que el individuo presente una plantilla igual a la guardada. Una serie de factores pueden influir en leves variaciones matemáticas, por ejemplo el peinado en los dispositivos lectores faciales. Para realizar la certificación, las plantillas deben ser similares entre sí en cierto grado. Esto no implica que los sistemas biométricos no sean seguros, sino que son sistemas probabilísticos, no absolutos. La exactitud de la medición varía de acuerdo a la tecnología y el fabricante, en valores desde 1/1,000 a 1/1078.

Técnicas biométricas

A continuación haremos mención de las principales técnicas biométricas utilizadas en seguridad:

Medición de huellas digitales

Después del ADN, las huellas digitales constituyen la característica humana más singular. La probabilidad de que dos personas tengan la misma huella digital es 1/67 billones. La medición automatizada de la huella digital requiere un gran poder de procesamiento y alta capacidad de almacenamiento.

Por esto, los productos biométricos basados en huella digital se basan en rasgos parciales, lo cual aumenta la posibilidad de que dos personas resulten con plantillas similares a valores entre 1/100,000 a 1/1,000,000, de los más seguros entre los dispositivos biométricos de seguridad.

Los dispositivos biométricos de huella digital son los más usados, a pesar de las aprensiones que tienen las personas en dar su huella digital. Son los productos con mejor precio, mayor cantidad de fabricantes y mayores ventas. Son convenientes y fáciles de usar.

Algunos dispositivos utilizan lectores de silicón, los cuales se deterioran con el uso del tiempo. Otros lectores de cámara son susceptibles a la suciedad y humedad de los dedos.

Por estas razones, los biométricos de huella digital son recomendados para instalaciones de alta seguridad pero de acceso restringido (casas, cuartos de cómputo, oficinas de funcionarios de alto nivel, etc.), computadoras y redes de cómputo.

Geometría de mano

Como su nombre lo indica, los biométricos basados en la geometría de la mano miden la forma de la mano por medio de una cámara infrarroja o visual. Ofrecen un buen balance entre la velocidad del análisis de las plantillas y facilidad de uso. Son ideales para uso masivo, como control de asistencia y acceso de entradas.

Su uso se ha incrementado en los últimos años. Sólo existen tres fabricantes en la actualidad.

Retina

Los lectores biométricos de retina analizan los capilares que están situados en el fondo del globo ocular. El usuario debe acercar el ojo al lector y fijar su mirada en un punto. Una luz de baja intensidad examina los patrones de los capilares en la retina. Este procedimiento es intimidante para algunos y hace de los lectores de retina los biométricos más impopulares, el usuario siente que su integridad física puede peligrar porque percibe un objeto extraño en su cuerpo, en ese caso la luz (esta característica no deseada de los lectores biométricos es conocida en inglés como intrusiva). Para que el lector pueda realizar su trabajo, el usuario no debe tener lentes puestos.

Iris

Los lectores de iris analizan las características del tejido coloreado que se encuentra alrededor de la pupila. Estos biométricos son los menos incómodos de usar de los lectores de ojo, porque no se realiza un contacto cercano con el lector. Además, es una de las tecnologías biométricas más exactas y el usuario puede usar los lentes al momento de la lectura. La facilidad de uso y la integración con otros sistemas no han sido puntos fuertes de los lectores de iris, pero se espera que mejoren con los avances técnicos.

Reconocimiento de cara

Los biométricos de reconocimiento de cara analizan las características faciales. Una cámara digital captura una imagen de la cara, a partir de la cual se crea la plantilla. El uso de esta tecnología es muy extendido en Europa. Es utilizada principalmente en aplicaciones de identificación. Los casinos los utilizan para identificar estafadores. Complejos comerciales y edificios los utilizan para identificar delincuentes y personas no gratas.

Lectura de firma

La técnica de verificación de firma analiza la manera que el usuario realiza su firma personal. Factores diversos, como la rapidez y presión, son cuantificados, así como la forma de la firma. La verificación tiene uno de los niveles más bajos de exactitud entre los lectores biométricos. Sin embargo, su familiaridad con los actuales procesos de verificación manual la hace una de las técnicas más fáciles de introducir al usuario.

Reconocimiento de voz

Los biométricos de reconocimiento de voz están basados en la verificación del patrón de voz. Su implementación puede ser económica si es realizada en computadoras, ya que la mayoría trae el hardware necesario: micrófonos y bocinas. Sin embargo, factores ambientales, como el ruido, pueden afectar la verificación. Además, el patrón del reconocimiento de voz es el que más espacio ocupa de todas las tecnologías biométricas, pudiendo llegar hasta 1 MB. Por estas razones, los biométricos de voz son percibidos por los usuarios como dispositivos poco amigables. La tecnología está siendo mejorada y se espera que en el futuro gane popularidad.

Usos de los biométricos

Los siguientes son los usos más comunes de los biométricos en los sistemas de seguridad:

Acceso físico

Por varias décadas, instalaciones de seguridad han utilizado la tecnología biométrica para los accesos de entrada. Actualmente es su uso principal: acceso a edificios y oficinas. Los biométricos permiten accesos seguros sin la presencia de un guardia de seguridad. Los biométricos de geometría de mano son los más usados en esta aplicación.

Acceso virtual

Actualmente, el método de seguridad más usado para el acceso a PCs y redes es la introducción de la contraseña. Sin embargo, la contraseña brinda una seguridad mínima para la protección de la información. Los precios de los biométricos han caído a un nivel en que permite su utilización para el acceso a redes y PCs. Esto brinda una mayor seguridad a los datos, porque la seguridad no está basada en lo que usted sabe, sino en quién es.

Asistencia

El control de asistencia es una de las aplicaciones en la cual los biométricos han tenido una gran acogida. Los biométricos son utilizados para la verificación de la asistencia, reemplazando los relojes de tarjeta. Esta es una aplicación donde el retorno de la inversión se refleja más claramente, porque las compañías se ahorran mucho dinero evitando el robo de tiempo, que se da cuando los empleados marcan con las tarjetas de otros.

Aplicaciones de comercio electrónico

Por muchos años, se ha aceptado la firma como el método para la verificación de la identidad de los dueños de tarjeta de crédito.

Sin embargo, está emergiendo con fuerza la utilización de biométricos con smart cards en los puntos de venta para la verificación de la identidad, brindado una seguridad muy superior. El comercio por Internet es mucho más crítico aún, porque no existe posibilidad de verificación de firma, la verificación se realiza contra lo que el comprador sabe. Varias compañías de tecnología han creado divisiones para el desarrollo de productos de software que permiten la utilización de biométricos para verificar quién es el comprador.

Vigilancia

Esta es una de las áreas de seguridad que presenta mayores retos para los biométricos. Utilizando reconocimiento de voz o de cuerpo, las compañías biométricas están desarrollando productos que permiten la identificación de sospechosos a edificios e instalaciones. Múltiples situaciones deben ser consideradas, como la identificación simultánea de varias personas y falta de consistencia en el ángulo, distancia y posición desde el lector.

Eligiendo biométricos

No es posible aseverar que una tecnología biométrica es mejor que otra. Cada una de las tecnologías tiene su aplicabilidad dentro de los sistemas de seguridad. Al momento de elegir biométricos, considere los siguientes factores:

Facilidad de Uso

Algunos dispositivos biométricos son más fáciles de usar que otros. Por ejemplo, los biométricos de mano utilizan guías para indicar la posición de la mano; en los lectores de cara puede ser difícil registrarse porque algunas personas tienen dificultad para alinear la cara en la posición correcta.

Factores que inciden en la lectura

Existen dos causas que pueden incidir en la ocurrencia de errores de la lectura: factores ambientales (ruido, iluminación, suciedad, clima, etc.) y condición del miembro corporal (cortaduras, desgaste, envejecimiento, etc.). Por ejemplo, la lectura de huellas digitales es susceptible a cortaduras, pero no cambia con el envejecimiento; el reconocimiento de voz es muy susceptible al ruido.

Precisión

Los fabricantes utilizan dos métodos para medir la exactitud de los biométricos: la tasa de falsa aceptación (FAR por sus siglas en inglés) y la tasa de falso rechazo (FRR). Ambos métodos se enfocan en la habilidad del sistema para permitir la entrada limitada de usuarios autorizados. Generalmente, los biométricos estáticos son más precisos que los biométricos de comportamiento.

Costo

Al momento de evaluar su cotización, considere los siguientes componentes de sistema que podrían ser utilizados:

- o Lector biométrico.
- o Capacidad de procesamiento necesaria para mantener la base de datos.
- o Instalación.
- o Implementación, incluya el entrenamiento.
- o Concienciación del usuario.
- o Mantenimiento del sistema.

Aceptación por el usuario

Mientras menos intimidante sea el biométrico, más rápidamente será aceptado. Los lectores de retina son muy poco aceptados, porque la luz inofensiva que proyectan en el ojo incomoda al usuario.

Estabilidad

Las compañías deben considerar la estabilidad de las tecnologías biométricas que evalúan. Factores que influyen en la estabilidad son: estandarización, madurez, años de investigación, soporte del gobierno y participación en el mercado.

Conclusión

La tecnología biométrica representa un área de los sistemas de seguridad que las compañías no pueden ignorar. Los biométricos incluyen una gama de características que benefician a dueños, empleados y clientes. Las compañías que adopten los biométricos en forma temprana gozarán de una ventaja competitiva. Sin lugar a dudas, su uso seguirá popularizándose.
