**Fundamentos Biométricos**

**Introducción**

Las nuevas tecnologías de seguridad confían en rasgos humanos únicos más que en *passwords* para salvaguardar datos sensibles.

Todos deseamos el acceso seguro a nuestros documentos, y sistemas sensibles, pero la inconveniencia y las limitaciones técnicas de las medidas de seguridad electrónica tradicionales tienen todos sus puntos débiles.

La tecnología que ha entusiasmado al espionaje y a programas de ciencia ficción en el último siglo es la seguridad biométrica. Esta tecnología hace uso del hecho de que cada persona tiene rasgos físicos únicos y específicos. Mientras que las novelas de detectives y las investigaciones policiales nos han hecho saber que nuestras huellas digitales son únicas, menos sabido es el hecho de que nuestros cuerpos son únicos en varias otras áreas también mensurables.

La tecnología biométrica utiliza esas particularidades para determinar nuestras identidades. La tecnología actúa como puerta de ingreso a los sistemas autorizados que requiera la autenticación exacta. Como por ejemplo el sistema podría ser una puerta de acceso con mecanismos de bloqueo electrónicos, un sistema operativo, o una aplicación donde los usuarios individuales tengan sus propios derechos y permisos. Por supuesto, esto es en parte, lo que han hecho los *passwords* por siempre, toda la vida, forever.

Los *passwords* determinan identidad con conocimiento del usuario. Si el usuario sabe el *password*, entonces puede acceder al sistema. La problemática es que un *password* no tiene relación alguna con su identidad real. Los *passwords* pueden ser robados, y los usuarios pueden dar sus *passwords* a otros, dando por resultado que el sistema se abra también a otros usuarios. No existe una manera infalible de hacer sistemas protegidos por *passwords* totalmente seguros de la intrusión desautorizada. Ni hay manera para que los sistemas basados en *passwords* determinen la identidad del usuario con certeza absoluta.

**Cómo Trabajan Los Sistemas Biométricos**

Una forma muy simple de describir el funcionamiento de un sistema biométrico es mencionar que estos sistemas consisten de hardware y software; el hardware captura la característica saliente del ser humano, y el software interpreta los datos que resultan y determina la aceptabilidad. “El paso crucial en la construcción de un sistema biométrico eficaz es el registro inicial. Durante el registro inicial, cada usuario, comenzando con el

administrador que controla el sistema, proporciona muestras de una característica biométrica específica al sistema”. Por ejemplo, el usuario coloca su dedo en un sensor soportado por un programa de lectura de la huella digital o se coloca delante de una cámara de video que puede capturar características del rostro u del ojo. El sistema después extraer las características apropiadas de la exploración y salva los datos como modelo. En una siguiente oportunidad, el usuario interactúa con el dispositivo biométrico otra vez, y el sistema verifica que los datos correspondan al modelo. Si el software no puede conseguir un “*matching*” adecuado, pueden ser necesarios más intentos, tal como el software de dictado aprende a reconocer los modelos del discurso del usuario en un cierto plazo. Una vez que este procedimiento sea completado, el sistema es operacional.

La próxima vez que el usuario intenta tener acceso al sistema, es explorado en esa característica biométrica específica (puede ser que se le pida proveer un nombre de usuario también), y el hardware pasa los datos al software, que controla los modelos de los usuarios. Si hay un “*matching*” , se le concede el acceso; si no, un mensaje señala que el

sistema no puede identificar al utilizador. Si se concede el acceso, se basa en su perfil de usuario. Si el usuario está intentando entrar a Windows 98 o NT, por ejemplo, el sistema abrirá como si se hubiera digitado el nombre de usuario y su *password*.

**Consideraciones Técnicas**

El cuerpo ofrece características reconocibles unívocamente en las siguientes áreas: huellas digitales, voz, ojos, manos, y cara. Es importante mencionar que diversos fabricantes están desarrollando productos alrededor de cada una de estas características. Las opiniones están divididas acerca de que tecnología es la mejor. El éxito se mide según un número de criterios, y cada tecnología tiene fuerzas y debilidades.

Los criterios más importantes se refieren a exactitud. El nivel de la exactitud en sistemas biométricos implica la tasa de falsa-aceptación y la tasa de falso-rechazo. La tasa de falsa-aceptación es el porcentaje de los usuarios que no están autorizados pero se les da acceso. La tasa de falso-rechazo es lo contrario, el porcentaje de los usuarios autorizados a los que se le niega el acceso. Estas tasas de exactitud son útiles, y los fabricantes de sistemas biométricos las citan a menudo en sus descripciones del producto. Pero no presentan un cuadro completo. El hecho es, los rasgos físicos de la gente cambian en un cierto plazo, especialmente con las alteraciones debido a accidentes o al envejecimiento. Además puede haber problemas debido a humedad en el aire, suciedad y sudor en usuario (en especial en sistemas que lean el dedo o mano). También, los usuarios de sistemas biométricos, deben ser entrenados para utilizarlos lo más eficientemente posible. Éstas y otras consideraciones limitan la exactitud de los dispositivos biométricos.

No existe duda que los sistemas biométricos son más exactos que otras clases de sistemas de seguridad, porque se basan en las características físicas reales de los usuarios, no en lo que saben (como con los *passwords*) o lo que están llevando (por ejemplo tarjetas de identificación). El éxito de la biométrica también se juzga mediante otros factores. La vulnerabilidad al fraude, también conocida como barrera para atacar, refleja cómo es probable que una persona pueda hacer un uso fraudulento del sistema mas allá de la seguridad. La estabilidad a largo plazo tiene en cuenta, por ejemplo si un sistema es útil para los usuarios muy infrecuentes, así como si las características de los usuarios se alteran en un cierto plazo. Otras medidas de la eficacia pueden incluir los factores que pudieron interferir con el sistema, facilidad de empleo, y la cantidad de espacio de disco que sus

datos toman.