Dispositivos biométricos

Seguramente en más de una ocasión hemos visto en los bancos, aeropuertos, hospitales, empresas o instituciones educativas personas que, para ingresar a una determinada área u oficina, aproximan su dedo, mano o rostro hacia un dispositivo, el cual, después de algunos segundos, les brinda o niega el acceso. Estos aparatos se denominan sistemas biométricos y son cada vez más frecuentes en la vida cotidiana. Su uso se ha extendido a computadoras personales y teléfonos celulares, de tal forma que para acceder a estos recursos es necesaria una autenticación, generalmente mediante la huella dactilar.

Pero ¿qué es la biometría? De acuerdo con el Subcomité en Biometría perteneciente al Consejo Nacional de Ciencia y Tecnología de los Estados Unidos (NSTC por sus siglas en inglés), la biometría es un término que se utiliza (a) para describir una característica, como una medición biológica (anatómica o fisiológica) o de conducta, empleada para realizar un reconocimiento automatizado; (b) como un proceso de reconocimiento de un individuo basado en características biológicas y conductuales que sean medibles. Es decir, consiste en la medición de ciertas características biológicas o de comportamiento que poseen todas las personas, pero que son únicas e irrepetibles en cada una de ellas, todo esto con el fin de llevar a cabo un proceso de reconocimiento, comprobando así que la persona es quien dice ser. La biometría se divide fundamentalmente en dos tipos: fisiológica (se nace con ella), como la huella dactilar, el rostro, la mano, el iris, la retina o los labios; y conductual (se adquiere), por ejemplo, la forma como un usuario teclea, la velocidad con la que firma o la manera como camina.

Con base en lo anterior, desde hace algunas décadas las empresas e instituciones preocupadas por la seguridad se han dado a la tarea de fomentar el empleo y desarrollo de equipos que, mediante el uso de la biometría, permitan identificar a las personas de forma más segura, rápida y eficiente. Es por ello que existen en el mercado innumerables dispositivos biométricos que satisfacen la necesidad de controlar el acceso físico a determinadas áreas o el acceso a los sistemas de información. Así pues, se tienen sistemas de reconocimiento de huella dactilar, iris, retina o geometría de la mano; sistemas de autenticación de patrones vasculares o características faciales; y sistemas de comportamiento, como los denominados dinámica de firma (Dynamic Signature Verification), ritmo de escritura (Keystroke Biometric System) o forma de caminar (Gait Biometry).

En términos generales, la manera como estos equipos registran e identifican a los usuarios es muy similar prácticamente en todas sus versiones.

El primer paso es el registro (*enrollment*), donde el dispositivo toma muestras de las características biológicas del usuario; posteriormente el sistema las convierte en una plantilla (*template*) y la almacena en una base de datos (no necesariamente como imagen, sino como una representación de esta); el siguiente paso es la identificación o "uno a muchos", donde el sistema biométrico identifica a la persona del resto de la población que ha sido registrada; y el último paso es la autenticación o "uno a uno". Aquí, el sistema hace coincidir la identidad de la persona con su biometría, complementando en ocasiones este proceso con el uso de otras tecnologías, como contraseñas, número de identificación personal o tarjetas.

Las ventajas de emplear un sistema biométrico son la facilidad de uso y la comodidad, ya que para identificar a un usuario bastará con que este se acerque o toque el dispositivo (según sea el caso); será más seguro y menos vulnerable a ataques por *software*, pues la complejidad y la especialización de estos sistemas reduce la posibilidad de *cracking*; y habrá poca probabilidad de pérdida o robo, dado que la clave de acceso es uno mismo.

Sin embargo, la utilización de este tipo de sistemas también representa ciertas debilidades, ya que no todos los dispositivos son igualmente confiables; por ejemplo, los sistemas de huella dactilar o escáner de iris son menos propensos a errores comparados con la dinámica de firma o reconocimiento de voz; hay sistemas que siguen siendo muy costosos, como los lectores de retina o iris; algunos son intrusivos, es decir, el usuario debe tener contacto físico con el dispositivo (como los lectores de huella dactilar o geometría de mano), lo que puede generar rechazo por considerarlos poco higiénicos. Asimismo, otra desventaja es que las lecturas pueden generar falsa aceptación (False Accept Rate o FAR), es decir, que un usuario no autorizado sea reconocido como válido, o falso rechazo (False Reject Rate o FRR), cuando un usuario autorizado sea rechazado.

A pesar de las dificultades que a lo largo de los años se han presentado en el desarrollo, la difusión y la aceptación de los dispositivos biométricos, seguramente en un futuro cercano el uso de contraseñas como método de acceso será obsoleto y hasta olvidado, y los procesos de identificación de usuario se realizarán a través de sistemas biométricos multimodales, es decir, adquisición de distintos rasgos biométricos (por ejemplo, huella dactilar y características faciales) que permitan aumentar la velocidad, eficiencia y confiabilidad, mejorando la manera en la que un usuario es reconocido.