

Sistemas de autenticación biométrica descentralizados.

Silvia Rentería¹, Artzai Picón¹, Estibaliz Garrote¹, Cristina Martínez¹

¹ Robotiker Tecnalía, Parque Tecnológico, Edificio 202. E-48170 Zamudio (Bizkaia)
(SPAIN)

Tel: +34 94 600 22 66, Fax: +34 94 600 22 99
{silvia, apicon, egarrote, cristina, }@robotiker.es

Abstract. En este artículo, se presenta, la investigación llevada a cabo por Robotiker-Tecnalía en el ámbito tanto del diseño como del desarrollo de nuevas arquitecturas para la autenticación de usuarios mediante técnicas biométricas. En él se explican los problemas inherentes a la utilización de sistemas de autenticación centralizados, presentando posteriormente una arquitectura descentralizada que muestre las ventajas de permitir utilizar e integrar cualquier tipo de sensor biométrico, y que a la vez proporcione características de seguridad y privacidad en las fases de captura, procesamiento, y almacenamiento de los datos biométricos del usuario. La solución presentada, puede ser utilizada con cualquier sistema desarrollado anteriormente, evitando de esta forma problemas de manejo de datos no estándar, protocolos de comunicación,... Así mismo, se presentan las características principales, requisitos y problemas de las diferentes aplicaciones biométricas.

Keywords: Biometría, Terminales móviles, Arquitectura Descentralizada.

1 Introducción

Hoy en día es necesario recordar multitud de contraseñas: para el móvil, el ordenador, las tarjetas de crédito....Resultaría de gran utilidad poder contar con un sistema de acceso seguro sin necesidad de utilizar esas claves, un sistema capaz de saber quienes somos. Por otra parte las empresas demandan nuevos dispositivos que permitan aumentar los niveles de seguridad, a la vez que agilizar su uso por parte de los clientes finales, todo ello sin suponer un gran aumento de costes. Los sistemas biométricos ofrecen una solución a este problema.

La biometría es la disciplina que permite identificar a las personas basándose en características fisiológicas o de comportamiento. El reconocimiento a través de características fisiológicas se realiza a partir de las medidas físicas de partes del cuerpo humano (huellas dactilares, mano, iris). Mientras que las basadas en el comportamiento tienen en cuenta cómo realiza cada persona determinadas acciones (voz, firma, escritura en teclado).

2. Requisitos principales para aplicaciones biométricas

Antes de definir una arquitectura válida para la implementación e integración de sistemas biométricos, es necesario conocer los requisitos que toda aplicación biométrica debe cumplir.

2.1 Requisitos de seguridad

Los requisitos principales que debe cumplir son:

Robustez del sistema: Un sistema basado en autenticación biométrica, debe ofrecer la misma o mayor seguridad que los sistemas de identificación actuales. Por ejemplo, en el caso de tarjetas de crédito, una vez obtenido el elemento físico, la probabilidad de averiguar su código de acceso (PIN 4 dígitos) es de 10^{-4} .

Protección del dato biométrico: Existen dos modelos diferenciados en cuanto a dónde debe ser almacenada la característica biométrica: en bases de datos centralizadas o en dispositivos en propiedad del usuario.

2.2 Requisitos funcionales

Por el momento, no existe un método biométrico capaz de funcionar con todo tipo de usuarios. El reconocimiento facial no funciona bien con gemelos, el iris con personas albinas, por lo tanto, siempre debe permitirse un método de autenticación alternativo al biométrico en la arquitectura del sistema. Esto puede realizarse teniendo en cuenta los siguientes criterios:

Autenticación de usuario biométrica y no biométrica: el sistema debe ser capaz de confirmar la identidad del usuario utilizando métodos alternativos al biométrico. En estos métodos alternativos el sistema debe tener la posibilidad de autenticar una persona sin necesidad de características biométricas, manteniendo, como mínimo, las mismas características de fiabilidad y robustez que el método biométrico.

Sistema Multibiométrico y multidispositivo: De cara a la definición de una arquitectura descentralizada, el sistema debe permitir la integración de distintos tipos de dispositivos biométricos (PDA, Móvil, sistemas embebidos, PC) así como distintas características biométricas (huella, voz, escritura,...).

2.3 Requisitos de interoperabilidad

Los sistemas biométricos deben ser capaces de operar en diferentes entornos, en diferentes localizaciones geográficas, y con diferentes tipos de usuarios. La interoperabilidad viene definida por la capacidad de los subsistemas hardware (HW) y software (SW) de operar conjuntamente de forma natural, sin necesidad de conocer las operaciones internas de cada subsistemas en la arquitectura global del sistema. En el caso de interoperabilidad en aplicaciones biométricas, se presentan dos áreas críticas.

Interoperabilidad entre dispositivos biométricos: es necesario que cada dispositivo biométrico disponga de una arquitectura y protocolo de comunicación compatible, para permitir la comunicación del dispositivo biométrico con los sistemas externos. (Por ejemplo: estándar BioAPI.)

Interoperabilidad entre bases de datos: es el caso de grandes aplicaciones biométricas (control de aeropuertos a nivel internacional). Todos los sistemas interconectados, deberían compartir las mismas bases de datos de usuarios. Esto lleva a la necesidad de que exista una compatibilidad entre dichas bases de datos. (Por ejemplo: CBEFF (Common Biometric Exchange File Format)).

3 Alcance de las aplicaciones biométricas

Dada la gran diversidad de escenarios, las soluciones biométricas implementadas, pueden diferir considerablemente. Pese a ello, se puede proponer una clasificación general.

3.1 Soluciones orientadas a la aplicación.

Se pueden distinguir dos tipos:

Solución específica: Esta solución está diseñada para identificar al usuario para darle acceso a una tarea determinada. Estos datos identificativos del usuario, pueden ser un número de contrato, el numero de cliente,... Esta solución tiene la ventaja de que, en caso de que la información sea robada, solamente se verá afectado el servicio relacionado con la aplicación ya que no está relacionada con datos oficiales de identificación.

Soluciones abiertas: Esta aproximación, puede ser usada por diferentes tipos de aplicaciones con requisitos similares. Un ejemplo podría ser un sistema único de autenticación que diera acceso a diferentes servicios (instalaciones, servicios de pago, sistema de salud, carnet de conducir,...). Este sistema debería autenticar al usuario

localmente utilizando sus características biométricas y después debería enviar la información relacionada con el mismo (certificado o ID digital, DNI,...) al servicio que desea autenticar al usuario. El uso de este tipo de sistemas permite pasar de información de autenticación no oficial (datos biométricos) con información oficial ampliamente aceptada.

3.2 Solución Global

Esta solución, sería el equivalente a un DNI en ámbito nacional o a un pasaporte en el internacional, con autenticación biométrica. Tanto el sistema de autenticación, como las características biométricas, debería estar avaladas por alguna entidad pública. Este sistema debería estar basado en estándares internacionales y regulado por diferentes instancias y organismos públicos y oficiales para garantizar su validez. Dada la complejidad de la solución, tanto técnica (estandarización, seguridad, ...) y especialmente a las políticas y jurídicas (legislación, acuerdos internacionales,...), se trata de una solución de difícil implementación.

4 Problemas actuales del uso de la biometría en aplicaciones generales

Con la información anterior, se puede observar, que resulta complejo, implementar una solución biométrica a gran escala.

Las aplicaciones actuales de autenticación biométrica están basadas en sistemas centralizados que almacenan las características biométricas del usuario en una base de datos. Como no existe una identidad biométrica globalmente aceptada (como un DNI biométrico), estas bases de datos contienen datos biométricos específicos para aplicaciones concretas (en el mejor de los casos siguiendo un estándar). De esta forma, un usuario debe darse de alta y proporcionar su característica biométrica a cada una de las bases de datos de los sistemas. Así, el usuario debería registrarse en el banco, en su lugar de trabajo, en el sistema domótico de su hogar, en el sistema de identificación de su vehículo, en su teléfono móvil,...

De esta forma, al estar los datos biométricos del usuario en diversas bases de datos se plantean los siguientes problemas:

Obligación de protección de los datos de carácter personal: los datos biométricos se consideran datos personales privados, y están regulados a nivel nacional e internacional. En Europa, existen directivas invitando a los países miembros a regular estos temas. Algunas de las mas relevantes son:

- Directiva **95/46/EC**,
- Directiva **2002/58/CE**

Dificultad para romper el vínculo entre los datos biométricos y la persona en sí: esto supone que el robo de una característica biométrica, es más problemático que el robo de números de identificación (tarjeta de crédito, DNI,...) ya que ésta no se puede cambiar como se hace con los códigos. Además, muchos usuarios potenciales temen dejar su información biométrica en un sistema desconocido en el que sienten que no tienen controlar quien está usando su información y para qué.

5 Solución propuesta

5.1 Una aproximación diferente

Se propone una solución basada en una nueva filosofía, que permite una fácil integración de una solución biométrica con los sistemas de autenticación clásicos instalados actualmente (basados en claves, llaves o tokens).

La novedad de la solución propuesta, reside en el uso de un terminal móvil genérico (teléfono móvil, PDA,...) que permita la autenticación biométrica utilizando dispositivos integrados en dicho equipos móviles (cámara, micrófono, lector de huella...). Sobre esta estructura HW se define una arquitectura, en la cual se permite la autenticación del usuario sin necesidad de acceder a bases de datos externas. Los datos biométricos son capturados, procesados y almacenados de forma segura en el propio terminal, permitiendo la autenticación del usuario en una gran cantidad de sistemas de forma segura, sin necesidad de compartir su identidad biométrica con terceros.

5.2 Terminal móvil

La selección de la característica biométrica a utilizar y del terminal vendrá determinada por:

- Los sistemas disponibles en los dispositivos móviles.
- Capacidad de almacenamiento en memoria.
- Capacidad de procesamiento.

Las opciones que, en este momento, serían factibles son:

	Huella	Voz	Iris	Firma
Madurez	Muy alta	Alta	Alta	Media
Mejor tasa de falsa aceptación	10^{-8}	10^{-2}	10^{-10}	10^{-4}
Mejor tasa de falso	10^{-3}	10^{-3}	10^{-4}	10^{-4}

rechazo				
Escalabilidad	Alta	Media	Muy alta	Media
Sensor integrado en dispositivo móvil	Sensor de huella: móvil (raramente) PDA(incluido)	Micrófono : móvil (incluido), PDA(incluido)	Cámara: móvil (incluido) PDA (opcional)	Pantalla táctil móvil (raramente) PDA(incluido)
Tamaño del template	< 200 bytes	< 2K bytes	256 bytes	< 200 bytes.
Precisión	Alta	Alta	Muy alta	Alta
Facilidad de uso	Alta	Alta	Media	Alta
Robustez ante acceso fraudulento	Alta	Media	Muy Alta	Media
Grado de aceptación por usuario	Medio	Alta	Medio	Muy alta
Estabilidad en el tiempo	Alta	Media	Alta	Media
Interferencias	Suciedad, edad, sexo y raza,	Enfermedad (resfriados)	Uso de gafas	Imitables y cambiantes

5.3 Arquitectura del sistema

Teniendo en cuenta los requisitos expuestos, se presenta, una arquitectura centrada en el usuario, fácilmente integrable en sistemas preexistentes, y que garantiza que los datos biométricos obtenidos no son enviados a los sistemas centrales del proveedor de servicios.

La autenticación de usuarios propuesta requiere de la existencia de un elemento que identifique al usuario (como el login actual) para posteriormente poder autenticar esta identidad. De esta forma se presupone que cada terminal corresponde a una única persona, aunque puede darse el caso de que una misma persona disponga de más de un terminal (por ejemplo Móvil y PDA) en cuyo caso dos identificadores (los correspondientes a cada terminal) servirían como base para autenticar a la persona.

Elementos de la arquitectura

Usuario: define la identidad del usuario final.

- A través de sus características biométricas se pueden autenticar su identidad.
- Se identifica a través de quién es, no de lo que sabe.

Terminal Móvil: es el soporte físico del sistema de identificación: PDA, teléfono móvil,...

- Elemento HW que permite extraer la característica biométrica del usuario.
- Es capaz de realizar el procesamiento de la información biométrica.

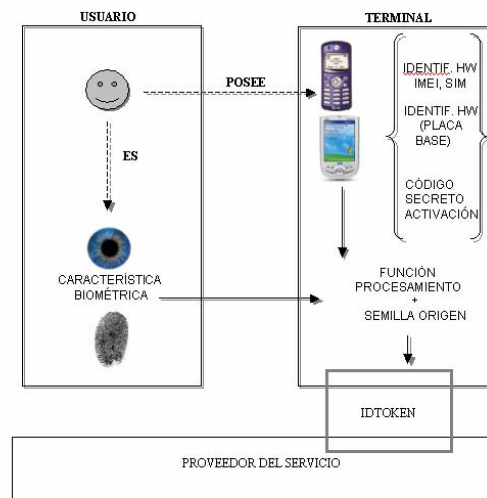
→ Los datos biométricos no son transmitidos a otros dispositivos, ni el dato capturado ni el template obtenido: menor riesgo de interceptación fraudulenta.

- Almacena el template de referencia
 - El template es obtenido con un algoritmo no reversible (a partir del template no se puede obtener el dato original)
- Tiene un identificador HW único (por ejemplo: código de la placa base).
 - Se utiliza como elemento de referencia del usuario.

Código Secreto de Activación: define un código que es enviado por el proveedor de servicio cuando el usuario se da de alta en el sistema. Su uso sería similar a la firma electrónica actual.

→ Se puede revocar en el momento que sea necesario.

A continuación se muestra un esquema simplificado del sistema.



Al autenticarse, se combinan los datos biométricos del usuario (1), el identificador del HW utilizado (2), así como el código de activación emitido por el proveedor de servicio (3).

Con estos tres datos, se genera un código (IDtoken) que es enviado al proveedor de servicio que identifica unívocamente al usuario, pero de tal forma que, no sea posible reconstruir ninguno de los tres datos utilizados para su generación a partir del mismo.

Una de las ventajas de la arquitectura propuesta, radica en que son necesarios los tres elementos para volver a generar el código requerido por el servidor. Ante cualquier sospecha de robo de alguno de los elementos, lo único que habría que hacer es reenrolarse en el servidor de tal forma que se varíe uno de los elementos generadores del código. De esta forma, el disponer de uno solo de los elementos generadores del código de identificación sería insuficiente para poder reconstruir la información.

6 Conclusión

A lo largo del artículo, se han presentado diferentes características, requisitos y problemas de las aplicaciones biométricas. Dentro de este marco, la solución presentada, ofrece las siguientes ventajas:

- Solo una única copia de las características biométricas es usada para cualquier número de servicios que requieran autenticación biométrica. De una simple característica biométrica se pueden obtener numerosos códigos de identificación electrónicos.
- Los datos biométricos se mantienen dentro del control del usuario, estos son capturados, procesados y almacenados dentro del propio terminal del usuario.
- No hay problemas de interoperabilidad entre sensores biométricos y bases de datos, ya que el usuario dispone de su propio terminal para la autenticación.
- Son utilizados dispositivos móviles genéricos.
- La solución es portable, de fácil implementación y uso.
- Los sistemas antiguos, pueden ser utilizados con pequeños cambios y manteniendo los códigos de identificación.