ANALISIS METODOLOGICO DE LA TECNOLOGIA TOUCHID BIOMETRICO

SEGURIDAD BIOMETRICA EN DISPOSITIVOS TOUCH ID

UNIVERSIDAD INTERNACIONAL DE LA RIOJA

Andrés palacios ortega
Ingeniero130@gmail.com

Contenido

INDICE DE ILUSTRACIONES

CAPITULO 1

INTRODUCCION

En este capítulo se mostrará una breve descripción del proyecto donde se describirá las causas y objetivos que han impulsado su desarrollo. Por último, se presentará un breve resumen que describe la estructura y contenido de la presente memoria.

1.1 MOTIVACION

Existen diversas casusas y motivaciones para realizar este proyecto, las cuales las orientaremos en dos partes.

Como punto de partida no hay que olvidar la normatividad de la huella biométrica, que se encuentra inmersa con el nuevo Reglamento de Protección de Datos en la Unión Europea GDPR (IBERLEY, 2017). Sin embargo, su obligatoriedad se ha postergado hasta el 25 de mayo de 2018, esta situación ha postergado avances significativos en la protección de lo datos de los usuarios desde el año 2016.

La evolución de la normativa comienza con la Directiva de 1995, la cual estableció un nuevo marco normativo común donde todos los usuarios disfrutarán de un mayor control sobre su información, a la vez que impone importantes cambios para las empresas. En el punto 1 del artículo 9 del Reglamento 2016/679 nos dice que los datos biométricos van a ser considerados como una categoría especial de datos personales y que, como regla general, estará prohibido su tratamiento, en particular, con una finalidad destinada a identificar de manera unívoca a una persona física.

Así, lo que establece dicho artículo en especial es lo siguiente:

“Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física,

datos relativos a la salud o datos relativos a la vida sexual o las orientaciones sexuales de una persona física” (Mañas, 2016).

Dicho lo anterior es de analizar el panorama actual de la tecnología TOUCH ID con las conclusiones que se recogen en la investigación realizada por IBM en el 2017 relacionadas con su seguridad, donde nos informa **“**USD 112 mil millones han sido robado a través de fraude de identidad, lo que equivale a USD 35,600 se perdieron en cada minuto. Cuantos más servicios hay ofrecido al público en general, con características de conveniencia y usabilidad que dependen de Internet, cuanto más amplia es la ventana de oportunidad para atacantes Javelin Strategy Research espera fraude relacionado con la creación de nuevas cuentas en línea aumentará hasta un 44 por ciento en 2018, aumentando pérdidas de USD 5 mil millones a USD 8 mil millones en cuestión de cuatro años**”** (Limor Kessem, 2017).

Comprobamos que, aunque existen múltiples estudios que analizan sus problemas de seguridad, ataques y mecanismos de protección asociados, no existen metodologías para cada uno de los elementos fundamentales involucrados en la huella dactilar y nos aporten el grado de cumplimiento de cada uno de los servicios de seguridad que integra esta tecnología de una forma objetiva, interrelacionando problemas de seguridad, ataques, mecanismos de protección y servicios de seguridad.

Por lo tanto, es recomendable diseñar una metodología que intente abordar esta problemática aportando soluciones objetivas, estableciendo valores concretos para cada uno de los aspectos de seguridad en función de los elementos de esta tecnología.

OBJETIVOS GENERALES

1. Analizar del panorama actual de la tecnología *TOUCH ID* y sus aplicaciones más comunes, haciendo especial mención a los elementos seguros (SE) y su gestión, así como su interrelación con la computación ubicua.

2. Desarrollar una metodología para evaluar la seguridad en TOUCH ID. Por tanto, detallaremos que elementos debemos tener en cuenta para conseguir una evaluación objetiva de seguridad de una tecnología como TOUCH ID. A continuación, se listan los aspectos principales para tener en cuenta en el desarrollo metodológico:

- Estableceremos los aspectos de seguridad fundamentales que cubre TOUCH ID. Esto significa una verificación de los niveles de seguridad mediante listas de verificación.
- Definiremos los problemas de seguridad que afectan a los diferentes elementos que componen la tecnología TOUCH ID. En este aspecto se definen algunas tablas de caracterización que permitan identificar las problemáticas más comunes del sistema de seguridad.
- Indicaremos los posibles ataques de los que pueden ser objeto cada uno de los elementos de la tecnología TOUCH ID.
- Concretaremos para cada uno de los ataques medidas de protección. Para este aspecto mediante controles de seguridad basados en la norma ISO/IEC 27001:2013 del cual obtendremos una matriz de riesgo en el anexo 1.

CAPITULO 2

2. MARCO TEORICO

TIPOLOGÍA DE LOS SENSORES ÓPTICOS Y DE ESTADO SOLIDO.

En este apartado se identifica los tipos de sensores más representativos y sus beneficios para el sistema de seguridad. De acuerdo con (UMANICK, 2013), los principales sensores se clasifican en sensores ópticos, de estado sólido y ultrasonidos, los cuales funcionan como sensores de seguridad para autenticación de usuarios. A continuación, se hace una descripción de los principales sensores.

SENSORES ÓPTICOS

a. FTIR (Frustrated Total Internal Reflection). Este sensor es una tecnología antigua y utilizada por los fabricantes. Consiste en que el dedo se coloca sobre un prisma de vidrio y se ilumina mediante una luz difusa. La diferente reflexión entre las crestas y los valles de la huella es recogida mediante un sensor CCD o CMOS que registrará la huella. Estos sensores proporcionan imágenes de buena calidad, pero no pueden miniaturizarse, ya que el tamaño del prisma es crítico si no se desean grandes distorsiones en la imagen obtenida

b. FTIR con prisma laminar. En este tipo de sensor es el encargado de reducir el tamaño del sensor FTIR clásico, se pule y de amolda la superficie interna del sensor en forma de micro prismas que hará creer que es el prisma de mayor tamaño. Las imágenes obtenidas por lo general son menores que las del caso normal.

c. Fibra óptica. Este sensor crea un arreglo de fibras ópticas de sentido vertical en donde el dedo entrara en contacto. La luz residual que es emitida por el dedo es recolectada por un sensor CCD/CMOS que se encarga de registrar la imagen y esta imagen tendrá una resolución tan alta como número de fibras haya.

d. Electro-ópticos. Estos sensores incorporan un tipo de polímero que, si se polariza, emitirá una luz en función del potencial que se encuentra en algún lado de sus caras. De este modo la diferencia de potencial que se crea por las crestas y los valles queda almacenada por un arreglo de fotodiodos o un sensor CMOS.

e. Lectura directa. Es una técnica que no requiere no requiere contacto directo con el sensor a diferencia de las otras ya mencionadas y solo basta con tomar una fotografía de excelente calidad de la huella y se debe procesar posteriormente para corregir distorsiones. Es muy complicado obtener estas imágenes de buena calidad y con buena resolución.

SENSORES DE ESTADO SÓLIDO

f. Capacitivos. Este método es el más común y más utilizado en la mayoría de dispositivos móviles en la actualidad. Este sensor está compuesto por un arreglo bidimensional de múltiples placas con pequeños condensadores. La superficie del dedo es un actor importante ya que es la segunda placa de los condensadores y dependiendo de la distancia la será diferente. Por consiguiente se puede conocer fácilmente las crestas de los valles. Uno de los principales problemas de estos sensores es su mantenimiento ya que el recubrimiento del sensor debe ser extremadamente fino y preciso. Estos sensores además pueden sufrir daños irreversibles al recibir descargas electrostáticas.

g. Térmicos. Estos sensores son fabricados con un material piro eléctrico. Los cambios en la temperatura entre las crestas, en contacto en la superficie, y los valles puede ser captada fácilmente. Adicionalmente estos son mantenidos a una temperatura relativamente alta para que el diferenciador sea mayor, por este

motivo se convierte en un factor importante ya que al lograr un equilibrio térmico la imagen desaparece. Una solución es que la huella se adquiera mediante barrido, es decir deslizar el dedo en una solo sentido por la superficie del sensor y manteniendo así la variación de temperatura. Estos sensores reducen el área de adquisición, se pueden integrar en sistemas portátiles y son muy resistentes a daños externos que los capacitivos.

h. Campo eléctrico. Estos sensores tienen incorporado un anillo el cual genera una señal eléctrica sinusoidal y una serie de antenas activas que recibe la señal modulada por la superficie del dedo el cual debe estar en contacto con el anillo y el sensor para un funcionamiento óptimo. La señal captada es amplificada, integrada y digitalizada para formar la imagen.

i. Piezoeléctrico. Son muy particulares ya que son muy sensibles a los campos eléctricos. La diferencia entre la presión que ejercen las crestas y los valles puede ser aprovechada para formar la imagen. Pero no se ha conseguido implementar sensores con la precisión suficiente con este tipo de sensor.

SENSORES DE ULTRASONIDOS.

Este tipo de sensores son comparables a una ecografía. Propagan señales acústicas a la superficie del dedo y captan la señal de eco recibida. Dicha señal de eco permite reconstruir la forma de la huella y la estructura de crestas y valles. Una ventaja es que es inmune a la suciedad y también a materiales que se interpongan entre el dedo y el sensor. Las desventajas que hacen que este sensor no haya proliferado es su complejidad, que hace difícil integrarlo en dispositivos de pequeño tamaño y aumenta su valor. La adquisición de las imágenes es, además, relativamente lenta.

3. ASPECTOS DE SEGURIDAD

En la tapa 1 de la metodología propuesta, el objetivo importante, es identificar los servicios o aspectos de seguridad, que garanticen la adecuada seguridad de los sistemas TOUCH ID y todos los elementos involucrados en su correcto.

La Seguridad Informática maneja tres pilares básicos importantes para la seguridad de la información, en particular, en lo relativo a la seguridad en Internet, o en redes de datos, o en la tecnología TOCUH ID. Estos son: confidencialidad, integridad y disponibilidad. Además, existen unos conceptos complementarios como autenticación, autorización, y no repudio.

IFigura 3.1 Pilares de la Seguridad.

La confidencialidad requiere que la información sea accesible únicamente por las entidades, sistemas o personas autorizadas. La confidencialidad de la información se aplica a todos los datos intercambiados por las entidades autorizadas o tal vez a sólo porciones o segmentos seleccionados de los datos, mediante cifrado. La confidencialidad de flujo de tráfico protege la identidad del origen y destino del mensaje.

La integridad requiere que la información solo pueda ser modificada por las entidades, sistemas, o personas autorizadas. La modificación incluye escritura, cambio, borrado, creación y reactivación de los mensajes transmitidos. La

integridad de la información asegura que los datos recibidos no han sido modificados de ninguna manera.

La disponibilidad significa que la información no puede obtenerse por parte de aquellos que están autorizados y la necesitan. Para lograr que la información esté disponible para estos que tienen que confiar en ella se utilizan mecanismos de autenticación y autorización.

La autenticación se encarga de probar que cada usuario es quien dice ser. Este aspecto requiere una identificación correcta del origen del mensaje, asegurando que la entidad o usuario no sean falsos.

Los sistemas se hacen mucho más seguros si esa autenticación no puede ser refutada después o sea, si el usuario no puede esquivar ninguna responsabilidad en las acciones que desarrolló dentro de un sistema.

Esto se conoce como no repudio de la identidad. Este ofrece protección a un usuario frente a otro que niegue posteriormente que en realidad se realizó cierta comunicación. El no repudio de origen protege al receptor de que el emisor niegue haber enviado el mensaje, mientras que el no repudio de recepción protege al emisor de que el receptor niegue haber recibido el mensaje.

La autorización se define como el proceso por el cual se determina qué, cómo y cuándo, un usuario autenticado puede utilizar los recursos de la organización. El mecanismo o el grado de autorización pueden variar dependiendo de qué sea lo que se está protegiendo. No toda la información de la organización es igual de crítica. Los recursos en general y los datos en particular, se organizan en niveles y cada nivel debe tener una autorización. Dependiendo del recurso la autorización puede hacerse por medio de la firma en un formulario o mediante una contraseña, pero siempre es necesario que dicha autorización quede registrada para ser controlada posteriormente.

En el caso de los datos, la autorización debe asegurar la confidencialidad e integridad, ya sea dando o denegando el acceso en lectura, modificación, creación o borrado de los datos. Por otra parte, solo se debe dar autorización a acceder a

un recurso a aquellos usuarios que lo necesiten para hacer su trabajo, y si no se le negará. Aunque también es posible dar autorizaciones transitorias o modificarlas a medida que las necesidades del usuario varíen.

De lo anterior, solo seleccionaremos los aspectos de seguridad fundamentales (confidencialidad, integridad y disponibilidad), además de los complementarios (autenticación, autorización, y no repudio), debido a su implicación inherente con TOUCH ID, como punto de partida de la propuesta metodológica.

3.1 PROBLEMAS DE SEGURIDAD

En la etapa 2 de la metodología, se pretende realizar un análisis exhaustivo, en base a la documentación científica existente, de todos los problemas de seguridad que engloba la tecnología TOUCH ID.

Una vez definidos los objetivos de esta fase, examinaremos los problemas de seguridad de los sistemas basados en TOUCH ID dependiendo de los experimentos desarrollados en dispositivos móviles en los sistemas operativos de Android y Apple.

Cuando analizamos estos sistemas biométricos de huella desde el punto de vista de la seguridad, teniendo en cuenta los tres modos de operación, nos podemos encontrar con los siguientes problemas de seguridad:

- Problemas de seguridad relacionados con las etiquetas.
- Problemas de seguridad relacionados con el sensor de huellas.
- Problemas de seguridad relacionados con la comparación de características
- Problemas de seguridad relacionados con la comunicación.

La figura 3.2. Muestra las secciones de la metodología donde se abordarán cada uno de los elementos implicados.

3.2 PROBLEMAS DE SEGURIDAD EN LAS ETIQUETAS TOUH ID

A diario dejamos nuestras huellas impresas en todas partes (lo que equivaldría a ir escribiendo nuestra contraseña cada vez que se abre una puerta, se coge un vaso, o nos sujetamos en el asidero de un autobús).

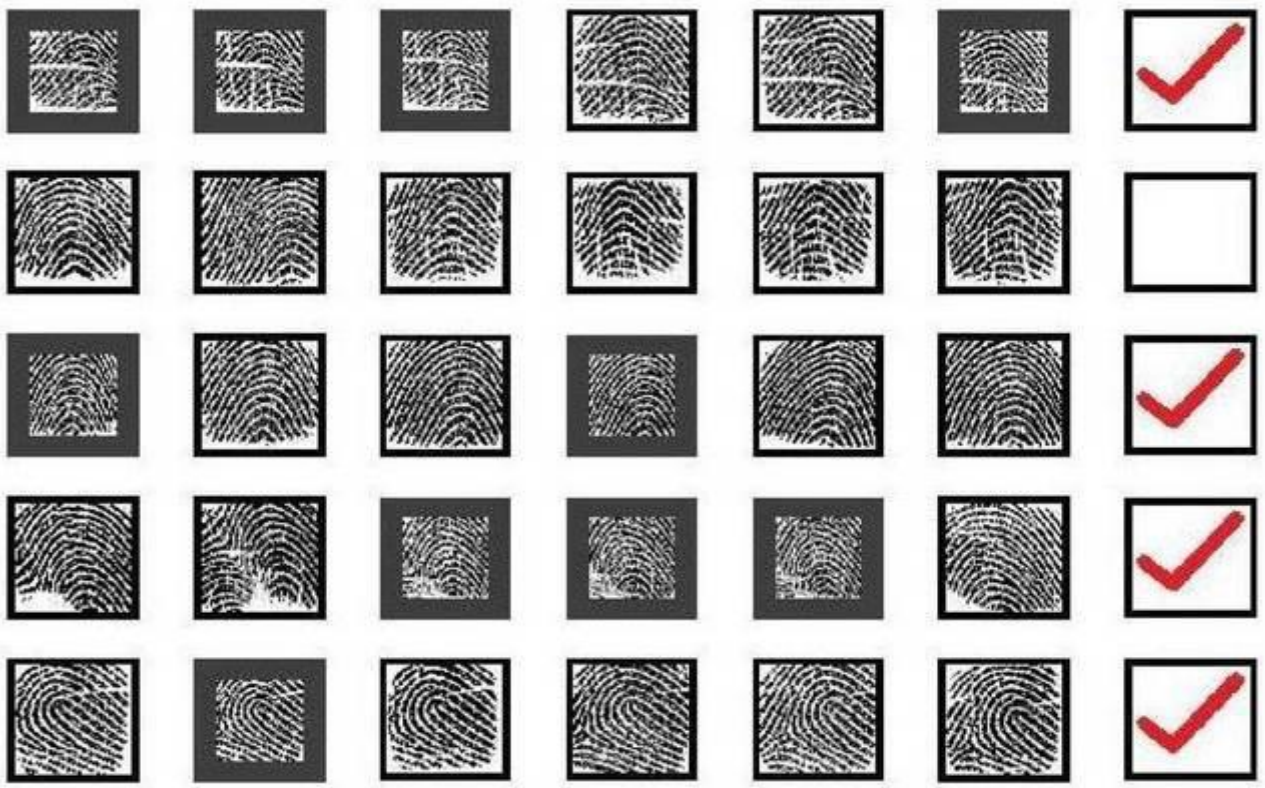
El modo de reconocimiento de huella involucra dos partes la huella dactilar y el escáner de huellas: es una etiqueta biométrica en un extremo, y el escáner del dispositivo móvil en el otro. Por lo tanto, para intentar suministrar seguridad en su conjunto, se debería considerar la seguridad de la etiqueta del escáner.

En base a lo anteriormente descrito, sería recomendable analizar primero los problemas de seguridad y los posibles ataques en las etiquetas de escáneres.

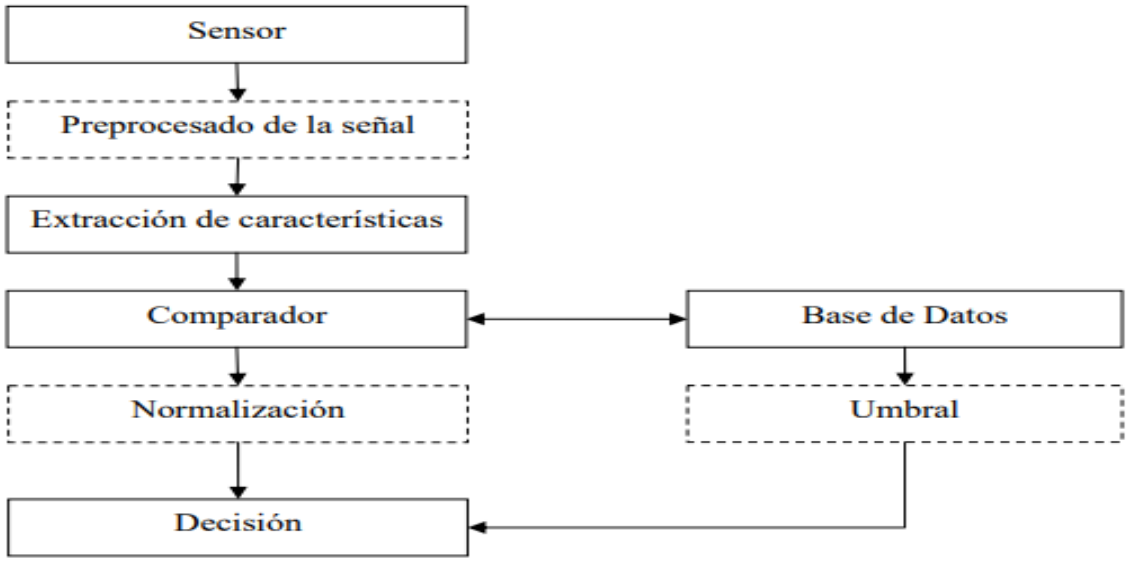
3.3 PROBLEMAS DE SEGURIDAD EN SENSOR DE HUELLA

Un estudio publicado por investigadores de la Universidad de Nueva York y de la Universidad de Michigan asegura que el sensor de huellas de nuestros móviles no es tan seguro como pensamos. A través de las pruebas realizadas por estos expertos, calculan que un teléfono móvil se podría desbloquear el 65 por ciento de las veces a través de unas 'huellas maestras', unos ejemplos que cuentan con las características más comunes de nuestras huellas digitales.

El motivo principal es que, dado el tamaño de los sensores digitales de nuestros móviles, **sólo tienen la posibilidad de realizar una lectura parcial de nuestras huellas** y no completa. Esta situación provoca que sea **más fácil encontrar una similitud** que permita acceder a un dispositivo movil. Y eso sin tener en cuenta que muchos usuarios cuentan con **varias huellas registradas**, bien del dedo pulgar e índice -los más comunes- o incluso de su pareja.



IIFigura 3.2 Registro Dactilar

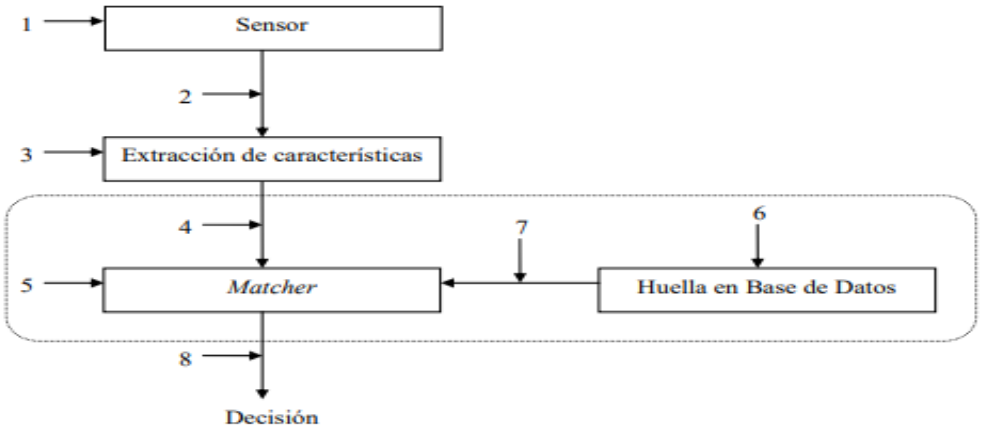


IIIFigura 3.2 Arquitectura de un sistema Biométrico.

3.4 PROBLEMAS DE SEGURIDAD EN LA COMUNICACIÓN

En todos los modos de operación de esta tecnología, se usa un rango de comunicación. Un atacante con huellas dactilares falsificadas o clonadas o con el uso de tarjetas inteligentes sin contacto y acceder al dispositivo. Por lo tanto, existe una probabilidad de ocurrencia de ataques y amenazas durante la comunicación en todos los modos de operación.

Se puede evidenciar un problema entre el canal del sensor y el extractor de características y puede ser interceptado y se puede introducir otra información que sustituya a la enviada por el sensor.



IVFigura 3.3 Posibles puntos de ataque a un sistema de reconocimiento biométrico (Ratha et al., 2001).

3.5 ATAQUES ELEMENTOS DE RECONOCIMIENTO BIOMETRICO TOCUH ID.

Como es habitual con todos los sistemas de información, los sistemas basados en pueden ser objeto de ataques que amenacen la seguridad del sistema y la privacidad del usuario.

El objetivo de esta tercera fase de la metodología propuesta es identificar cada uno de los posibles ataques a los que pueden enfrentarse los elementos que conforman la arquitectura Biométrica donde se considera un ataque como, una

violación a la seguridad del sistema derivada de una amenaza inteligente, es decir, un acto deliberado que intenta evadir los servicios de seguridad y violar las políticas de seguridad de un sistema.

Vamos a ir analizando los posibles ataques de los que pueden ser objeto los elementos fundamentales: etiquetas, sensores y la comunicación.

3.6 ATAQUES EN ETIQUETAS BIOMETRICAS TOUCH ID.

Examinaremos, a continuación, el comportamiento de una etiqueta biométrica cuando está en modo apagado. Los ataques comunes contra etiquetas pueden categorizarse como:

- Clonación y suplantación de etiquetas de huellas.
- Cambios en el contenido de la etiqueta de comparación de extracción de características.
- Reemplazo y ocultación de etiquetas en la base de datos.

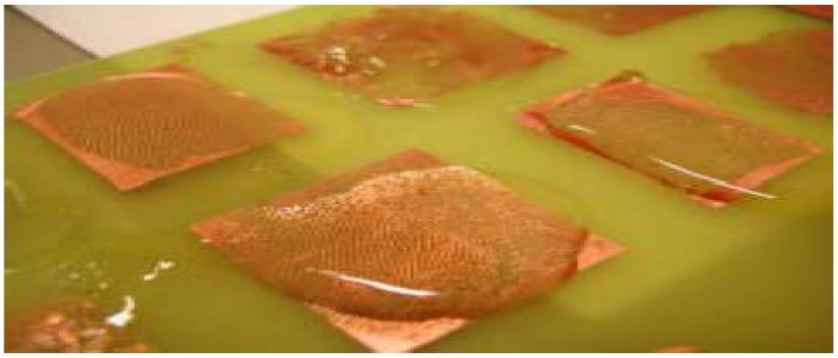
3.7 CLONACIÓN Y SUPLANTACIÓN DE ETIQUETAS DE HUELLAS.

En (J. Keuning., 2000) se realizó un experimentó con diferentes sensores para comprobar si se podía acceder al sistema con un dedo artificial de goma fabricado por ellos mismos a partir de uno real. Estos autores describen dos métodos para crear dedos artificiales: uno con cooperación de un usuario real y otro sin la cooperación del dueño del rasgo biométrico. Como cabe esperar, cuando se cuenta con la cooperación del dueño la calidad de la imitación es mayor y es más fácil lograr un ataque exitoso al sistema:

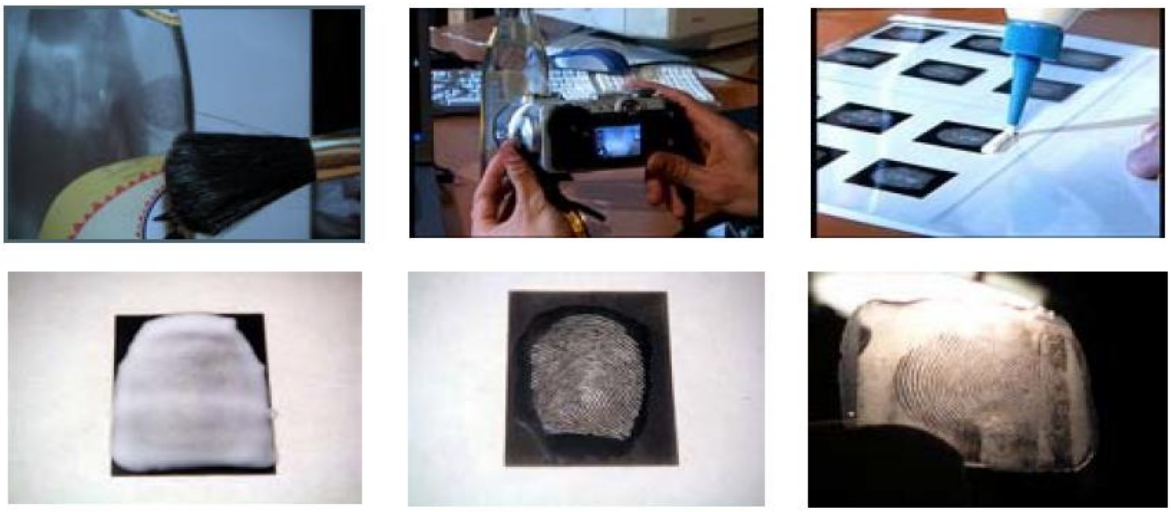
- **Con cooperación**: Estos autores crearon un molde de un dedo hecho con plastilina y relleno con una fina capa de silicona líquida para simular el dedo

falsificado. Ya con el dedo sólido, la extrajeron y perfilaron la yema del dedo de la persona que iba a atacar el sistema de manera que resultaba prácticamente indetectable.

- **Sin cooperación**: La obtención de la huella se realizó sobre una huella que deja el usuario presente por ejemplo en un vaso cuando toma vino. Posteriormente se espolvoreó con un polvo muy fino de con algún color coloreado luego se levanta por medio de cinta adhesiva. A continuación se toma una fotografía de la huella (con una cámara analógica convencional) y el negativo de esta se sitúa sobre una placa de prototipado PCB (Printed Circuit Board). Se debe exponer la placa con el negativo encima a rayos ultra violeta y someterla a un baño de ácido ya con esto la huella queda perfectamente marcada sobre la superficie de la misma. A partir de la huella de la PCB y empleando silicona líquida se logró obtener una réplica de la huella tal como se puede observar en la Figura 3.4.



VFigura 3.4 Obtención de huellas de silicona a partir de un PBC.



VIFigura 3.5 Fases del proceso de imitación de huella con cola de madera (Kàkona, 2001).

En la figura 3.5 se definen las fases por la cual se obtiene una huella falsa en primer lugar la huella es realzada con un polvo de grafito y a partir de ella poder obtener una imagen digital e imprimirla en un papel transparente mediante una impresora láser, y con ayuda del tóner generar un pequeño relieve. Después de tener esto se debe cubrir con pegante para madera y esperar a que seque para poder despegarla de la hoja. Como último obtendremos la falsificación completa teniendo la huella dactilar de la persona.

Por otra parte [((T. Matsumoto, 2002))] llevo a cabo ataques muy similares a lo antes expuesto solo que esta vez utilizó gelatina en vez de silicona, utilizo el método de cooperación por parte de los dueños, los dedos de gelatina fueron aceptados por los 11 sistemas a estudio con una probabilidad de entre el 68% y el 100%, y al no haber cooperación el porcentaje de aceptación de los 11 sistemas fue siempre superior al 67%.

De acuerdo a todas estas pruebas de ataques contra los sensores de huellas y como se reconstruyen para ser clonadas o falsificadas (Kàkona, 2001) elaboro una metodología la cual se basa en la reconstrucción de fragmentos de huella capturados sin colaboración para crear una huella completa después imprimirla y presentarla a un sensor óptico. También presentó otra forma de atacar esos sistemas capacitivos empleando el aliento sobre la superficie del sensor.

Así se puede evidenciar una huella latente del usuario anterior ya que el vapor del aliento y la grasa latente de la huella anterior provocan que el sensor se active.

También (L. Thalheim, 11/2002) a través de sus experimentos sobre diversos sensores de huella que son comerciales con ataques por medio de dedos falsos. Demostró que es posible obtener la huella de un usuario anterior en un sensor capacitivo empleando el aliento, utilizando solo cinta adhesiva y polvo de grafito o tan solo presionando a través con una bolsa de plástico llena de agua. Utilizo las técnicas que se expusieron en los apartados anteriores sobre los tipos de sensores térmicos y el cual se comprobó que son los más complicados de atacar ya que incluso con huellas de silicona, la imagen resultante es de muy baja calidad.

Para finalizar esta serie de experimentos y demostraciones (J. Galbally-Herrero, October 2006) creó una base de datos de huellas de silicona y documentado su eficiencia frente a distintos tipos de sensores. Estudio cómo la eficiencia de los ataques está condicionada por el tipo de sensor utilizado por ejemplo si se emplea un sensor óptico las tasas de éxito son superiores a diferencia de otros sensores. Se utilizan dos sistemas de verificación, uno basado en minucias y otro en texturas. El sistema basado en minucias presentó un rendimiento global mejor, aunque el basado en texturas fue más robusto frente a los ataques.

3.8 CAMBIOS EN EL CONTENIDO DE LA ETIQUETA DE COMPARACION DE EXTRACCION DE CARACTERISTICAS.

En (Soutar., 2002) propone un ataque Hill Climbing (equivalente a “subida a la montaña”) donde el objetivo es un sistema básico de reconocimiento de imágenes el cual se basa en correlación de filtros. Los templates o patrones sintéticos se van introduciendo gradualmente al sistema de autenticación se utiliza las puntuaciones que devuelve el sistema de comparación, este autor demostró que mediante sucesivas variaciones del template o patrones, se puede lograr una incorrecta identificación. Este ataque se le denomina ataque Hill Climbing ya que a partir de las puntuaciones devueltas por el comparador se generan imágenes nuevas

artificiales que elevan las sucesivas puntuaciones. Este método puede clasificarse como un ataque de comparación de extracción de características.

El método Hill Climbing se aplica como un ataque al sensor (antes del extractor de características) no es importante poseer información del modo en el cual se almacenan los templates o patrones, lo que es absolutamente necesario para un ataque de comparación.

Por otra parte (U. Uludag, January 2004) y (A.K. Jain A. R., 2004) implementaron un ataque de comparación utilizando la misma técnica dela ataque Hill Climbing el cual emplea conjuntos de características generadas sintéticamente conociendo previamente el formato de almacenamiento de los templates.

El ataque descrito por estos dos autores es el de introducir sucesivos conjuntos de minucias generadas mediante algoritmos que se van a ir modificando a lo largo del ataque.

En el algoritmo de ataque se desconoce la información del patrón del usuario concreto que se desea suplantar, es decir se conoce cómo se almacena la información pero no cuál es la información.

Por otra parte utiliza las puntuaciones devueltas por el comparador y las características de minucias sintéticas, el ataque tratará de generar nuevos grupos de minucias y de estas puntuaciones sean mayores que las anteriores en un ciclo hasta lograr un resultado alto como para superar el umbral y lograr la verificación positiva.

3.9 REEMPLAZO Y OCULTACIÓN DE ETIQUETAS.

Pegar una etiqueta de huella maliciosa encima de la etiqueta original o reemplazar la etiqueta original con una etiqueta maliciosa, es suficiente para dejar al sistema funcionando como el atacante desea.

En el primer caso, además, es posible deshabilitar la etiqueta original. Otro método para atacar etiquetas pasivas es romper la protección de escritura de una etiqueta y sobrescribirla con datos maliciosos.

3.10 ATAQUES AL SENSOR DE HUELLAS.

Pueden existir muchos ejemplos en actualidad de ataques hacia los rasgos biométricos falsos y presentarlos al sensor. Lo cual nos muestra la veracidad y certeza de esta clase de métodos para romper la seguridad de cara al sensor.

Pueden estudiarse las falencias de estos sensores de reconocimiento de huella dactilar en función al tipo de sensor que se desea utilizar. Siendo probable que el gran desarrollo de los sistemas dependa de la calidad de las imágenes porque su rendimiento depende de esto.

En la actualidad existe software que lo realiza, como SFinGe (Synthetic Fingerprint Generator) donde permite atacar, al igual que el ataque de Hill Climbing, y no requieren imágenes de huellas dactilares.

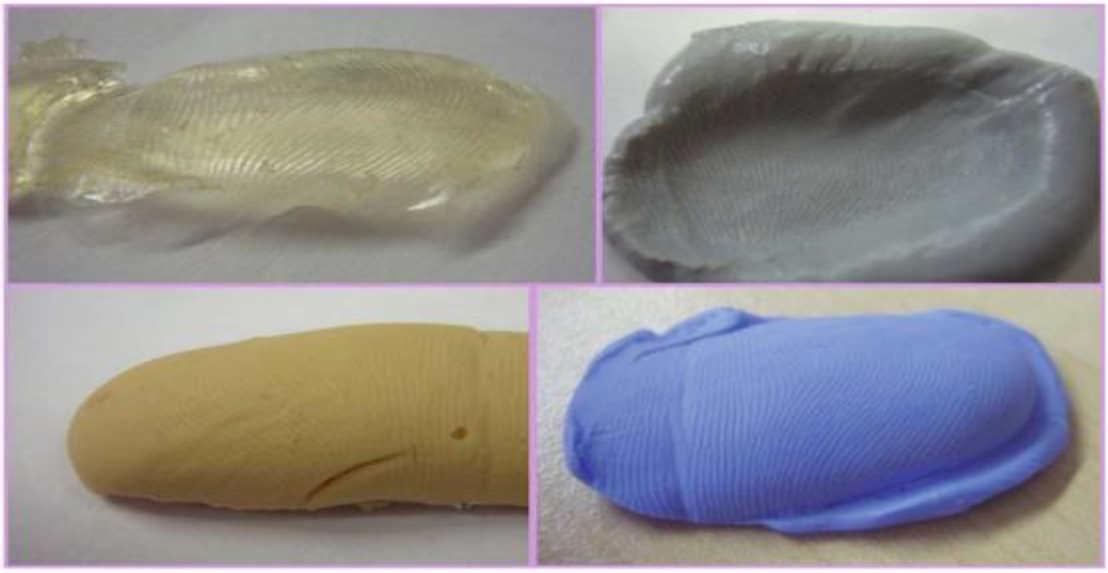
Un atacante puede tratar de destruir el sensor, posteriormente crear una huella a partir de una que haya dejado el usuario o tan solo simplemente una imagen de una huella que se pretende suplantar.

VIIFigura 3.6 Ataque a iPhone mediante huella en plastilina

Como podemos observar en la figura 3.6 como con un trozo de plastilina podemos acceder al dispositivo móvil.

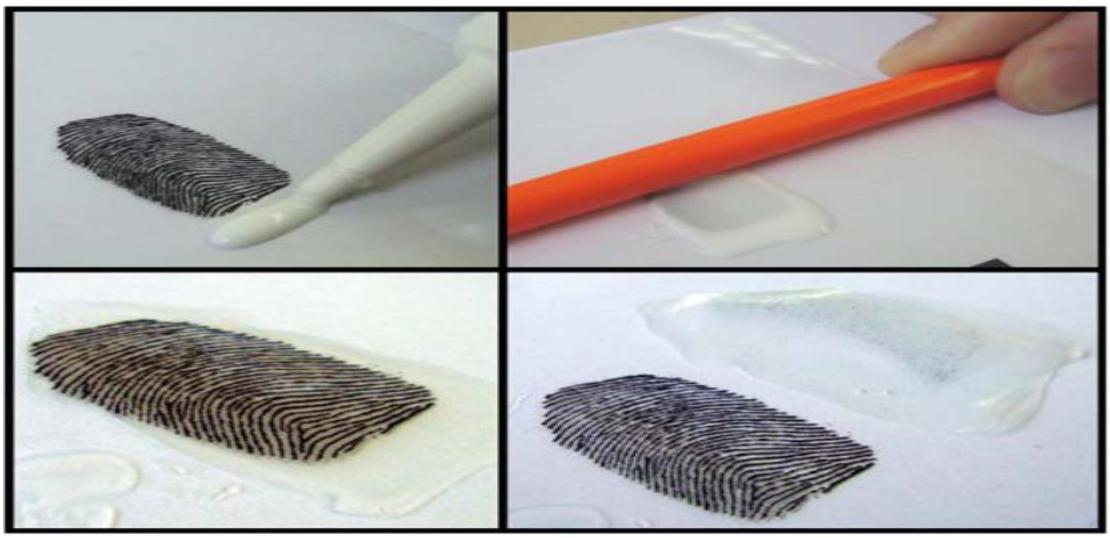
Algo que no sólo ocurre en sistemas de huellas dactilares de dispositivos móviles, sino que también es posible en el resto de sensores actuales. El motivo la resolución con la que los sensores actuales trabajan, creando imágenes de 500-550 puntos por pulgada (dpi), un detalle que como pudimos ver es insuficiente para que el teléfono distinga entre la huella auténtica y la falsa.

Esta comprobación vino de la mano de Vkansee, una empresa china que presentó un proyecto relacionado con mejorar este aspecto de los actuales sensores de huellas en el CES 2015. Su propuesta de hecho se basa en la creación de unos sensores cuya imagen obtenida es de mayor resolución, concretamente de 2.000 dpi, evitando que la huella falsa pueda ser interpretada como buena al obtener un detalle cuatro veces mayor.



VIIIFigura 3.7 Huellas clonadas o falsificadas

El ataque al sensor como podemos observar se puede reconstruir una huella de la víctima y con tener acceso a su dispositivo y a toda la información que allí este expuesta.



IXFigura 3.8 Pegamento de madera con una huella dactilar impresa como negativo.

Como se muestra en la figura 3.8 los posibles ataques que se pueden realizar al sensor muy fácilmente dejando al descubierto toda nuestra información.

3.11 ATAQUES CONTRA LA COMUNICACIÓN.

(Soutar., 2002) propone este ataque Hill Climbing o subida a la montaña de un sistema de reconocimiento de imágenes que se basa en la correlación de filtros. Este ataque utiliza los patrones sintéticos que se van almacenado al sistema de autenticación. Utiliza todas las puntuaciones la cual nos devuelve el sistema de comparación, este autor demostró que con las variaciones repetitivas de los patrones, se puede lograr una identificación errónea.

- El Hill Climbing cuando lo enfocamos hacia extractor de características no es necesario tener información del modo de almacenamiento del patrón, lo que es absolutamente necesario para un ataque de comparación.
- Los autores Uludag y Jain en el 2004, implementan un ataque hacia el comparador donde se utiliza la técnica de Hill Climbing que emplea conjuntos de características generadas sintéticamente ya sabiendo el formato en el cual se almacenan los patrones posteriormente introduce repetitivos conjuntos de minucias generadas mediante algoritmos los cuales se modificaran a lo largo del ataque, en este algoritmo no se conoce la información del patrón del usuario el cual se va a suplantar. Ya con las puntuaciones obtenidas por el comparador y las características de estos conjuntos de minucias sintéticas, según la lógica del ataque generara nuevos grupos de minucias cuyas puntuaciones sean mayores que las anteriores así repetitivamente hasta lograr un resultado alto superar el umbral y que dicha validación sea positiva.

3.12 MECANISMOS DE DEFENSA

En de aclarar que en algunos de los ataques antes descritos, existen recomendaciones para que se pueden integrar en cada uno de los elementos afectados por parte del atacante.

En la cuarta etapa de la metodología propuesta, el objetivo principal es seleccionar los múltiples mecanismos de seguridad que pueden implementarse, con la

finalidad de reforzar la seguridad de uno o varios elementos involucrados en la arquitectura biométrica de los sistemas de huella dactilar, y que permitan prevenir ataques a la seguridad, detectarlos o saber recuperarse de ellos.

3.13 MECANISMOS DE DEFENSA EN ETIQUETAS TOUCH ID.

Según los ataques descritos anteriormente ya para que dichos ataques tengan éxito siempre necesitara la puntuación obtenida en el comparador, por eso es necesario realizar un algoritmo el cual proteja al comparador y nunca revele la puntuación y que simplemente solo de la aceptación o rechazo por parte del sistema.

Por otra parte (Soutar., 2002) según sus estudios y experimentos los cuales hemos conocido a lo largo del documento llega la conclusión y propone cuantificar las puntuaciones devueltas por el comparador para protegerse del ataque Hill Climbing.

La ventaja que se tiene, ya que el ataque se basa en pequeñas modificaciones de la plantilla inicial, ya que al mejorarlos o emporarlos no podrán ser detectados al permanecer la mejoría dentro del mismo paso de cuantificación y mantenerse invariable la puntuación de salida. Es de anotar que todo comparador se puede considerar de forma cuantificada, las puntuaciones se encuentran entre los valores 0 y 100 y sólo puede tomar valores enteros.

Esta cuantificación deberá ser, en consecuencia, lo muy atrevida que sea muy útil como medida de protección.

3.14 MECANISMOS DE DEFENSA EN SENSONRES DE HUELLA TOUCH ID

Ya como hemos observado clonar o falsificar una huella es muy sencillo y hace que un sensor de huellas sea vulnerable y puedan acceder a nuestra información personal muy fácil y con el objetivo de evitar este ataque se recomienda el uso de dos factores en el proceso de autenticación.

Para ello se puede utilizar biometría bimodal (dos técnicas biométricas diferentes, por ejemplo huella dactilar e iris, etc.), o combinar la biometría con el uso de contraseña y/o tarjetas de identificación**.**

3.15 MECANISMOS DE DEFENSA EN LA COMUNICACIÓN.

Si bien es cierto el refrán que dice más vale prevenir que lamentar es sin duda la comunicación entre el extractor de características y el comparador e inclusive la base de datos donde se almacena esta información y cuyo objetivo principal protegerla a toda costa.

Para ello es recomendable:

- cuantificar las puntuaciones devueltas por el comparador como un método de protección ante ataques Hill Climbing.
- Encriptar la puntuación de salida para que no se pueda conocer su valor real.
- Restringir el número de intentos de acceso al sistema por parte de un mismo usuario en un cierto periodo de tiempo.

CAPITULO 4

METODOLOGIA DE ANALISIS DE RIESGOS DE UN TOUCH ID

A lo largo de este capítulo se realizarán las investigaciones oportunas para conseguir de forma oportuna la manera de evaluar metodológicamente esta tecnología. Para lograr hacer esto a lo largo de este capítulo se irá dando estructura. Por lo tanto, en primer lugar, se definirá la metodología y luego iremos desarrollándola.

4.1 DESCRIPCION DE LA METODOLOGIA

Como punto de partida se deben detallar que elementos se deben tener en cuenta para lograr una evaluación objetiva de seguridad. Se deben incluir todos los aspectos de seguridad fundamentales, y que estos sean el centro del estudio. Por lo tanto, estableceremos los conceptos de confidencialidad, integridad y disponibilidad, además de autenticación, autorización, y no repudio, asociados a esta tecnología, que posteriormente deberemos evaluar en base al resto de actividades.

Una vez establecidos los aspectos de seguridad a evaluar, definiremos los problemas de seguridad que afectan a los diferentes elementos que componen esta tecnología, fundamentalmente, etiquetas, sensor de huellas, elemento seguro y comunicación.

Se detallarán los posibles ataques de los que pueden ser objeto cada uno de los elementos mencionados, indicando los aspectos de seguridad que afectan. Para cada uno de los ataques, se definirán medidas de protección, cuando sea posible para intentar evitar los posibles efectos negativos sobre el sistema.

Por último, con base a lo expuesto, se darán de forma objetiva a cada uno de los aspectos de seguridad planteados un valor (bajo, medio, alto) individual, que en su conjunto definirán la seguridad aportada.

A continuación, se mostrara una tabla resumen de la metodología, que ilustra cada los objetivos y cada una de las actividades requeridas.

Objetivos	Actividades
1. Analizar del panorama actual de la tecnología *TOUCH ID* y sus aplicaciones más comunes, haciendo especial mención a los elementos seguros (SE) y su gestión y el impacto que tiene sobre el sistema si se materializa un ataque.	Listar los ataques más comunes de hacia los sensores biométricos en dispositivos móviles basados en la norma ISO 27001, e identificar su mecanismos de defensa.
2. Desarrollar una metodología para evaluar la seguridad en TOUCH ID. Por tanto, para cada riesgo encontrado en el objetivo 1 se tendrá evaluación objetiva de seguridad de una tecnología como TOUCH ID basados en la norma ISO 27001.	La evaluación, parte final de esta metodología propuesta, será llevada a cabo aplicando los resultados obtenidos en cada uno de los riesgos encontrados, obteniendo para cada servicio de seguridad, y cada elemento TOUCH ID involucrado un valor cuantitativo**.**

XTABLA 3.1 Metodología Propuesta.

4.2 RIESGOS DE LA TECNOLOGIA TOUCH ID.

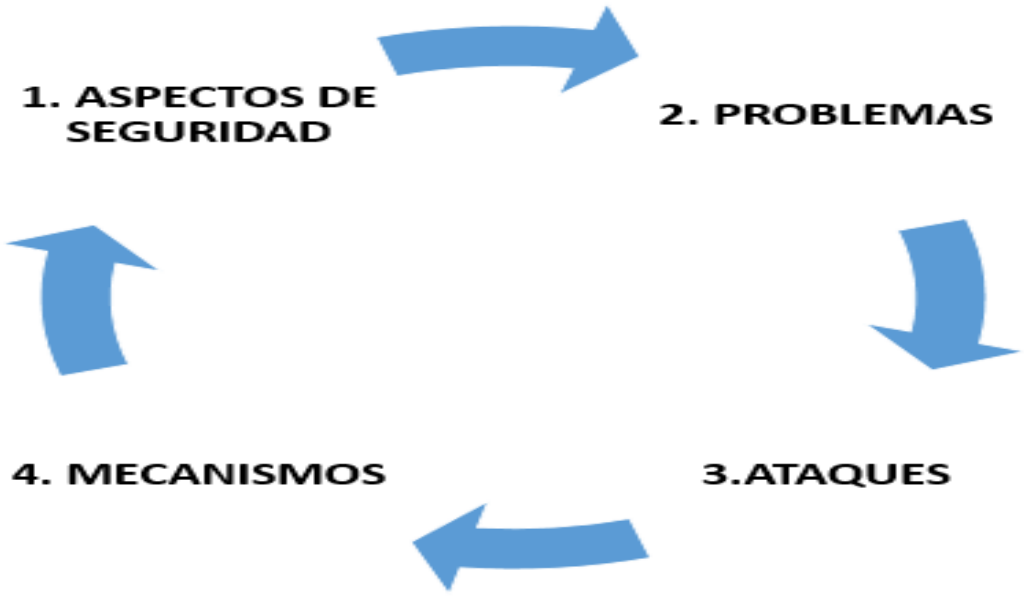
En este punto se darán valores para cada uno de los aspectos de seguridad que marcan la seguridad de sensores biométricos de huella dactilar, para dar este valor se tendrá en cuenta la información aportada hasta este punto, de una manera objetiva hasta plasmar la realidad de la seguridad en unos valores acotados de cumplimiento.

La evaluación, parte final de esta metodología propuesta, será llevada a cabo aplicando los resultados obtenidos en cada una de las fases previas, obteniendo

para cada servicio de seguridad, y cada elemento involucrado un valor cuantitativo.

Para la evaluación propuesta en esta metodología, se aprovecharan las diferentes implicaciones que existen entre las distintas etapas, las etapas dos y tres se interrelacionan con la primera, dado que los problemas de seguridad, de manera pasiva, y los ataques, de manera activa, influyen directamente en los aspectos de seguridad.

La etapa cuatro se relaciona directamente con el resto de etapas. El siguiente grafico muestra las interrelaciones existentes entre las diferentes fases de la metodología.



XI**Figura 3.9 Relaciones que existen en las diferentes fases de la metodología.**

Basados en la norma ISO/IEC 27001:2013 en cual en su anexa A nos indica que controles de seguridad se deben tener en cuenta al momento de implantar alguna tecnología hacia un usuario final.

Se toman de esta lista 20 controles de seguridad los cuales el fabricante puede tener en cuenta para el desarrollo de la tecnología TOUCH ID, se proponen métodos para el analizar la vulnerabilidad y una solución de acuerdo al control de seguridad.

LISTA DE RIESGOS BASADOS EN LA NORMA ISO 27001

Algunas de las amenazas más comunes son las siguientes:

a). Perdida de la Información.

b). Corrupción o modificación de la información.

c). Sustracción, alteración o pérdida de equipos o componentes.

d). Divulgación de la información.

e.) Interrupción de servicios.

a). POLITICA DE CONTROL DE ACCESO

CONTROL 1. El fabricante debe establecer, documentar y revisar una política de control de acceso basada en los requisitos de negocio y de seguridad de la información.

En este control es importante que el fabricante siempre documente y este alineado con una política de control de acceso ya definida pavimente con esto se garantiza que el control se seguridad se cumpla.

Para lograr que el control tenga éxito se debe realizar un método para poder analizar la vulnerabilidad de este control esto con el fin de tomar acciones correctivas y mitigar el riesgo al que se encuentre expuesto.

METODO PROPUESTO

El fabricante debe ponerse en modo atacante puede tratar de destruir el sensor, presentar una huella latente o una imagen de la huella que pretende suplantar. También pueden fabricarse huellas de goma o silicona para imitar otra huella.

Con esto el fabricante asegura que la política de control de acceso sea un poco más segura y mitigar el riesgo que se puede generar si no se tiene encuentra esta validación pueden acceder terceros sin problema al sistema

SOLUCION PROPUESTA.

Se propone esta solución para proteger un sistema de esta clase de ataques primero es importante que el comparador nunca revele la puntuación de la huella sino simplemente la indicación de aceptación o rechazo por parte del sistema.

Esta solución es viable en ciertos casos, como en algunos sistemas embebidos, pero para los que empleen varios rasgos biométricos (sistemas multimodales), la puntuación debe ser conocida por otros elementos del sistema y por lo tanto puede ser visible.

b). ACCESO A LAS REDES A LOS SERVICIOS DE RED

CONTROL 1. El fabricante debe proporcionar a los usuarios el acceso a las redes y a los servicios en red para cuyo uso hayan sido específicamente autorizados.

En este control es importante que el fabricante proporcione los accesos y servicios de la redes a sitios seguros con el fin de alertar al usuario si se encuentra en algún sitio no seguro y que puede poner en riesgo el sistema.

Para lograr que el control tenga éxito se debe realizar un método para poder analizar la vulnerabilidad de este control esto con el fin de tomar acciones correctivas y mitigar el riesgo al que se encuentre expuesto.

METODO PROPUESTO

El fabricante debe ponerse en modo atacante se puede medir la transluminancia del dedo, detectando la luz que atraviesa el dedo o la reflexión de la luz en el dedo mediante un emisor y un receptor luminoso. Mediante una fotopletismografía se puede medir el pulso cardiaco a través de la detección de la variación del volumen de sangre que circula por el dedo.

Con esto el fabricante asegura que solo a través de una huella real se pueda tener el acceso a las redes y sitios seguros.

SOLUCION PROPUESTA.

Se propone esta solución para proteger al sistema de huellas falsificadas por eso es importe que el sensor este en el ranking de los mejores en el mercado que permita conexiones a redes de Wifi seguras y así brindar una comunicación más segura con el usuario.

c). REGISTRO Y BAJA DE USUARIO

CONTROL 1. El fabricante debe implantar un procedimiento formal de registro y retirada de usuarios que haga posible la asignación de los derechos de acceso.

En este control es importante que el fabricante proporcione los accesos al sistema mediante un procedimiento previamente elaborado donde permita conceder o revocar los derechos de acceso para un usuario para ello tanto el sensor como el comparador deben asegurar que la persona que está accediendo sea el dueño dela información.

Para lograr que el control tenga éxito se debe realizar un método para poder analizar la vulnerabilidad de este control esto con el fin de tomar acciones correctivas y mitigar el riesgo al que se encuentre expuesto.

METODO PROPUESTO

El fabricante en modo de atacante debe proteger el canal el cual puede ser interceptado y se puede introducir otra información que sustituya a la enviada por el sensor y allí tener acceso al sistema.

SOLUCION PROPUESTA.

Para proteger el sistema frente a estas amenazas el fabricante debe emplear el mejor algoritmo de encriptación y emplearlo en el canal de comunicación así le será más difícil al atacante poder descifrar los puntos de la huella.

d). PROVISION DE ACCESO DE USUARIO

CONTROL 1. El fabricante debe implantar un procedimiento formal para asignar o revocar los derechos de acceso para todos los tipos de usuarios de todos los sistemas y servicios.

En este control es importante que el fabricante proporcione los accesos al sistema mediante un procedimiento previamente elaborado donde permita conceder o revocar los derechos de acceso para un usuario para ello tanto el sensor como el comparador deben asegurar que la persona que esta accediendo sea el dueño dela información.

Para lograr que el control tenga éxito se debe realizar un método para poder analizar la vulnerabilidad de este control esto con el fin de tomar acciones correctivas y mitigar el riesgo al que se encuentre expuesto.

METODO PROPUESTO

El fabricante en modo de atacante y con cooperación del usuario se obtiene de una huella latente de un usuario en un vaso de vidrio. En primer lugar se espolvoreó con un fino polvo coloreado para posteriormente levantarla por medio de cinta adhesiva. A continuación tomaron una fotografía de la huella (con una cámara analógica convencional) y situaron el negativo sobre una placa de prototipo de PCB (Printed Circuit Board). Después de exponer la placa con el negativo encima a rayos ultra violeta y someterla a un baño de ácido la huella

queda perfectamente marcada sobre la superficie de la misma. A partir de la huella de la PCB y empleando de nuevo silicona líquida se pudo obtener una réplica de la huella.

SOLUCION PROPUESTA.

Para proteger el sistema de este tipo de ataques el fabricante debe proporcionar que los sensores de huella so sean suplantados y dar recomendaciones al usuario para que este se mas precavido de donde deja sus huellas dactilares ya que ingenuamente puede ser víctima de un ataque.

e). GESTION DE PRIVILEGIOS DE ACCESO

CONTROL 1. La asignación y el uso de privilegios de acceso debe estar restringida y controlada por el fabricante.

En este control es importante que el fabricante proporcione los accesos necesarios al sistema y debe estar controlada para que los usuarios no puedan acceder y realizar cambios del sistema ocasionado fallos o quedando vulnerable a posibles ataques.

Para lograr que el control tenga éxito se debe realizar un método para poder analizar la vulnerabilidad de este control esto con el fin de tomar acciones correctivas y mitigar el riesgo al que se encuentre expuesto.

METODO PROPUESTO

Este método se realiza directamente a la base de datos del sistema de reconocimiento biométrico. En él, utilizando un comparador de huella comercial, se realiza ingeniería inversa sobre el patrón de datos de las minucias y se generan las imágenes artificiales correspondientes a las huellas dactilares interceptadas.

En este tipo de ataques estarían además contemplados los casos en los que el atacante tuviera acceso privilegiado a la base de datos o al canal de comunicación entre el comparador y la base de datos.

SOLUCION PROPUESTA.

Para proteger el sistema de este tipo de ataques es necesario que el fabricante tenga un buen conocimiento en el formato concreto en que se almacenan los patrones en la base de datos y los pueda modificar introduciendo nuevos patrones, cambiando o eliminando alguno ya existente para que los patrones que se almacenen en la base de datos sean más seguros.

f). GESTION DE LA INFORMACION SECRETA DE AUTENTICACION DE USUARIOS

CONTROL 1. La asignación de la información secreta de autenticación debe ser controlada a través de un proceso formal de gestión definida por el fabricante.

En este control es importante que el fabricante proporcione y exija siempre la una autenticación segura por parte del usuario y así evitar vulnerabilidades a posibles ataques y perdida de información.

Para lograr que el control tenga éxito se debe realizar un método para poder analizar la vulnerabilidad de este control esto con el fin de tomar acciones correctivas y mitigar el riesgo al que se encuentre expuesto.

METODO PROPUESTO

En este método el fabricante debe utilizar una huella a través con polvo de grafito para realzar la huella para después obtener a partir de ella una imagen digital e imprimirla en papel de transparencia con una impresora láser, cuyo tóner genera un pequeño relieve. A continuación se cubre con cola para madera y se espera a que seque para posteriormente despegarla de la hoja. La falsificación queda así completa.

SOLUCION PROPUESTA.

Para proteger el sistema de este tipo de ataques el fabricante debe adoptar un scanner que permita realizar un doble factor de autenticación que si se logra acceder mediante una huella falsificada obligue a la autenticación con otro método de autenticación por ejemplo con el iris y una contraseña alfanumérica etc.

g). REVISION DE LOS DERECHOS DE ACCESO DE USUARIO.

CONTROL 1. Los propietarios de los activos deben revisar los derechos de acceso de usuario definidos por el fabricante a intervalos regulares.

En este control es importante que el fabricante dentro de la programación de autenticación del TOUCH ID en su derechos de acceso el fabricante reduzca el número de intentos de 5 a 3 ya que con esto reduce la posibilidad de que el atacante tenga éxito, posterior a ello deberá pedir al usuario una contraseña alfanumérica para lograr acceder al sistema y así evitar vulnerabilidades a posibles ataques y perdida de información.

Para lograr que el control tenga éxito se debe realizar un método para poder analizar la vulnerabilidad de este control esto con el fin de tomar acciones correctivas y mitigar el riesgo al que se encuentre expuesto.

METODO PROPUESTO

En este método el fabricante debe centrarse directamente a la extracción de características para ello debe utilizar un algoritmo seguro y realizar pruebas mediante las técnicas de comparación, como por ejemplo la de minucias o basadas en alineamiento de patrones y así poder determinar qué tan difícil es para al atacante acceder al sistema.

SOLUCION PROPUESTA.

Para proteger el sistema de este tipo de ataques el fabricante debe tener un buen algoritmo de encriptación, como se ha mencionado anteriormente está en la base fundamental para que un atacante le sea más difícil acceder al sistema es por ello que el fabricante no debe reducir costos al momento de implantar una tecnología como esta en donde la información es el actor principiar de esta cadena.

h). RESTRICCION DEL ACCESO DE LA INFORMACION

CONTROL 1. El fabricante debe restringir el acceso a la información y a las funciones de las aplicaciones, de acuerdo con la política de control de acceso definida.

En este control es importante que el fabricante debe asegurar que no se pueda alterar el código y atacantes no puedan acceder a otras aplicaciones del dispositivo o puedan instalar software malicioso.

Para lograr que el control tenga éxito se debe realizar un método para poder analizar la vulnerabilidad de este control esto con el fin de tomar acciones correctivas y mitigar el riesgo al que se encuentre expuesto.

METODO PROPUESTO

El fabricante deberá basarse en técnicas basadas en correlación este método sirve para hacer el cálculo de correlación entre la imagen de muestra y la de entrada tratando de maximizarla Cuanto mayor sea la correlación mayor será la similitud entre las huellas a comparar y su maximización permitirá calcular el valor del desplazamiento y la rotación que hacen que las dos imágenes sean lo más parecidas posibles.

SOLUCION PROPUESTA.

Para proteger el sistema de este tipo de ataques el fabricante debe implementar un sistema detector de intrusos que ponga alerta el sistema y no permita que a través de imágenes puedan acceder a nuestro sistema.

h). PROCEDIMIENTOS SEGUROS DE INCIO DE SESION

CONTROL 1. Cuando así se requiera en la política de control de acceso, el acceso a los sistemas y a las aplicaciones se debe controlar por medio de un procedimiento seguro de inicio de sesión definido por el fabricante.

En este control es importante que el fabricante realice un procedimiento de inicio de sesión seguro que obligue al usuario a relaizar una autenticación segura con dicho procedimiento.

Para lograr que el control tenga éxito se debe realizar un método para poder analizar la vulnerabilidad de este control esto con el fin de tomar acciones correctivas y mitigar el riesgo al que se encuentre expuesto.

METODO PROPUESTO

El fabricante deberá basarse en técnicas basadas en minucias son los más conocidos y de uso más extendido en la actualidad. Están basados directamente en la forma en que los expertos forenses realizan la comparación entre huellas. En este caso la representación es un vector de características de longitud variable cuyos elementos son las minucias de la huella. Cada minucia se puede describir a partir de un número de atributos como su posición en la imagen, su orientación, tipo (final de cresta o bifurcación de cresta), un peso basado en la calidad de la imagen en su vecindad, etc. La mayor parte de los algoritmos basados en minucias consideran cada singularidad como una tupla (,) x y θ indicando la posición horizontal y vertical de la minucia y su orientación en la imagen.

SOLUCION PROPUESTA.

Para proteger el sistema de este tipo de ataques el fabricante debe implementar un sistema donde aparte de la autenticación por TOCUH ID debe tener un factor doble de autenticación en nuestro sistema.

i). SISTEMA DE GESTION DE CONTRASEÑAS

CONTROL 1. Los sistemas para la gestión de contraseñas deben ser interactivos y establecer contraseñas seguras y robustas definidas por el fabricante.

En este control es importante que el fabricante realice un procedimiento de inicio de sesión seguro que obligue al usuario a realizar una autenticación segura con dicho procedimiento.

Para lograr que el control tenga éxito se debe realizar un método para poder analizar la vulnerabilidad de este control esto con el fin de tomar acciones correctivas y mitigar el riesgo al que se encuentre expuesto.

METODO PROPUESTO

El fabricante deberá basarse en técnicas basadas en patrones de crestas o texturas se describe una técnica basada en texturas locales en la que el área de la huella se subdivide en zonas con respecto al núcleo de la huella. Se calcula un vector de características basado en la información de cada zona resultante de la subdivisión.

SOLUCION PROPUESTA.

Para proteger el sistema de este tipo de ataques el fabricante debe implementar un sistema donde aparte de la autenticación por TOCUH ID debe proteger el sistema con un algoritmo de encriptación muy seguro para las puntuaciones y no sea tan fácil lograr descifrarlas.

j). USO DE UTILIZADES CON PRIVILEGIOS DEL SISTEMA

CONTROL 1. El fabricante debe restringir y controlar rigurosamente el uso de utilidades que puedan ser capaces de invalidar los controles del sistema y de la aplicación.

En este control es importante que el fabricante proteja la arquitectura del sistema mediante algoritmos seguros y siempre se estén actualizando para que al atacante le quede muy difícil acceder al sistema los algoritmos hash más recomendables actualmente para proteger las contraseñas son los siguientes:

- scrypt (KDF)
- bcrypt
- Argon2 (KDF)
- sha512crypt
- sha256crypt
- PBKDF2 (KDF).

Para lograr que el control tenga éxito se debe realizar un método para poder analizar la vulnerabilidad de este control esto con el fin de tomar acciones correctivas y mitigar el riesgo al que se encuentre expuesto.

METODO PROPUESTO

El fabricante deberá impedir que el atacante conozca alguna parte de la arquitectura del sistema de autenticación biométrica y/o tiene privilegios de acceso. Este hecho condiciona su facilidad de aplicación con respecto a los ataques al sensor. En cambio, no precisan crear modelos físicos de la huella sino que se deberá disponer de conocimientos acerca de la parte software del sistema.

SOLUCION PROPUESTA.

Para proteger el sistema de este tipo de ataques el fabricante debe implementar un procedimiento el cual se defina que algoritmo puede ser el mejor para utilizar y realizar pruebas de intrusión para comenzar a evaluar que tan seguro es como todo sistema no se puede garantizar que sea 100% seguro pero si una alta dificultad de poder acceder al sistema.

k). CONTROL DE ACCESO AL CODIGO FUENTE DE LOS PROGRAMAS

CONTROL 1. El fabricante debe restringir el acceso al código fuente de los programas.

En este control es importante que el fabricante proteja el código fuente de esta tecnología mediante algoritmos seguros jamás se deben almacenar las contraseñas en texto en claro ya que los ciberdelincuentes obtendrán fácilmente todas las claves sin necesidad de crackearlas por esto se debe utilizar el mejor algoritmo de encriptación para que el atacante le sea muy difícil acceder y tener acceso al código fuente.

Para lograr que el control tenga éxito se debe realizar un método para poder analizar la vulnerabilidad de este control esto con el fin de tomar acciones correctivas y mitigar el riesgo al que se encuentre expuesto.

METODO PROPUESTO

El fabricante deberá utilizar mediante algún software o programa intentar acceder al código fuente y a través de este programa suplantar al extractor de características a modo de troyano y enviar características generadas a voluntad del atacante al comparador.

SOLUCION PROPUESTA.

Para proteger el sistema de este tipo de ataques el fabricante debe restringir el acceso al código fuente del sistema para evitar posibles ataques de código malicioso que puedan generar fallos del sistema y suplantaciones de identidad y puedan acceder al sistema.

Por otra parte el fabricante nunca debe permitir que el comparador revele la puntuación sino simplemente la indicación de aceptación o rechazo por parte del sistema. Esta solución es viable en ciertos casos, como en algunos sistemas embebidos, pero para los que empleen varios rasgos biométricos (sistemas multimodales), la puntuación debe ser conocida por otros elementos del sistema y por lo tanto puede ser visible.

l). POLITICA DE USO DE LOS CONTROLES CRIPTOGRAFICOS

CONTROL 1. El fabricante debe desarrollar e implementar una política sobre el uso de los controles criptográficos para proteger la información.

En este control es importante que el fabricante desarrolle una política para el uso de controles criptográficos para las aplicaciones TOUCH ID ya que mediante este método de autenticación podría acceder a información muy sensible para el usuario.

Para lograr que el control tenga éxito se debe realizar un método para poder analizar la vulnerabilidad de este control esto con el fin de tomar acciones correctivas y mitigar el riesgo al que se encuentre expuesto.

METODO PROPUESTO

El fabricante deberá utilizar el método de ataque Hill Climbing donde el objetivo principal es el de atacar directamente el comparador y no utiliza información alguna de la imagen de la huella. Emplea exclusivamente patrones sintéticos de minucias generados aleatoriamente o según una distribución que se estime aproximada a la huella, basada en histogramas de minucias de las huellas de una base de datos. Únicamente es necesario conocer cuál es el sensor, para así saber cuál es su resolución y el tamaño de las imágenes que genera.

SOLUCION PROPUESTA.

Para proteger el sistema de este tipo de ataques el fabricante se debe cuantificar las puntuaciones devueltas por el comparador como un método de protección ante ataques Hill Climbing. La ventaja de esta medida es clara, puesto que al basarse el ataque en pequeñas modificaciones de la plantilla inicial, una leve mejora o un leve empeoramiento no podrán, en general, ser detectados al permanecer la mejoría dentro del mismo paso de cuantificación y mantenerse por lo tanto invariable la puntuación de salida.

m). GESTION DE CLAVES

CONTROL 1. El fabricante debe desarrollar e implementar una política de sobre el uso, la protección y la duración de las claves de cifrado a lo largo de todo su ciclo de vida.

En este control es importante ya que el fabricante desarrolle una política para el uso claves de cifrado de esto dependerá la seguridad de esta tecnología debe obligar al usuario a cambiar sus claves periódicamente pues esto puede minimizar los ataques que puedan ocurrir.

Para lograr que el control tenga éxito se debe realizar un método para poder analizar la vulnerabilidad de este control esto con el fin de tomar acciones correctivas y mitigar el riesgo al que se encuentre expuesto.

METODO PROPUESTO

El fabricante deberá utilizar un método en el cual le permita reactivar la huella de un usuario anterior y en un sensor capacitivo empleando el aliento, utilizando una cinta adhesiva con polvo de grafito o presionando con una bolsa de plástico fina llena de agua y apoyándose también junto con las técnicas descritas anteriormente (minucias, patrones de crestas o texturas etc.) intentar lograr acceder al sistema.

SOLUCION PROPUESTA.

Para proteger el sistema de este tipo de ataques el fabricante mediante la política de gestión de claves debe obligar al usuario cambiar sus claves de acceso periódicamente, por ejemplo ir utilizando cada una de las huellas de sus dedos con esto podrá minimizar posibles ataques.

n). CONTROLES CONTRA EL CODIGO MALICIOSO

CONTROL 1. El fabricante debe implementar los controles de detección, prevención y recuperación que sirvan como protección contra el código malicioso, así como procedimientos adecuados de concienciación al usuario.

En este control es muy importante ya que el fabricante debe desarrollar e implementar controles de detecciones IDS que protejan el sistema contra ataques de código malicioso y permitan detectar actividades inapropiadas, incorrectas o anómalas desde el exterior-interior de un sistema informático.

Para lograr que el control tenga éxito se debe realizar un método para poder analizar la vulnerabilidad de este control esto con el fin de tomar acciones correctivas y mitigar el riesgo al que se encuentre expuesto.

METODO PROPUESTO

El fabricante deberá crear una base de datos de huellas de silicona y documentar su eficiencia frente a distintas clases de sensores determinar cómo la eficiencia de los ataques está condicionada por el tipo de sensor utilizado.

En el caso de emplear un sensor óptico se evidencian que las tasas de éxito son superiores que en el caso de otros sensores, el fabricante debe utilizar dos sistemas de verificación, uno basado en minucias y otro en texturas y establecer cuál de los dos sistemas presenta un mejor rendimiento y cual es más robusto frente ataques de códigos maliciosos que intentan acceder al sistema.

SOLUCION PROPUESTA.

Para proteger el sistema de este tipo de ataques el fabricante no debe utilizar sensores baja calidad ya que esto puede ocasionar muchos fallos de seguridad al usuario todo lo contrario debe utilizar lo último en tecnología para poder ofrecer al usuario ese plus adicional en el producto de que puede estar tranquilo y que es muy difícil que un atacante pueda acceder a su información personal. Es importante que el fabricante mantenga al usuario actualizado y concientizarlo de utilizar los procedimientos adecuados definidos previamente en la tecnología TOCUH ID y se ciña a lo estipulado por el fabricante.

ñ). REGISTRO DE EVENTOS

CONTROL 1. El fabricante debe registrar, proteger y revisar periódicamente las actividades de los usuarios, excepciones, fallos y eventos de seguridad de la información.

En este fabricante debe desarrollar e implementar un registro de eventos de fallos del sistema donde se almacenen los accesos que realiza el usuario puede ser de la última semana para tener un registro histórico.

Para lograr que el control tenga éxito se debe realizar un método para poder analizar la vulnerabilidad de este control esto con el fin de tomar acciones correctivas y mitigar el riesgo al que se encuentre expuesto.

METODO PROPUESTO

El fabricante deberá crear una base de datos y establecer los periodos de tiempo en que registraran los log del sistema contra fallos o posibles ataques con el fin de saber la fecha y la hora en que ocurrieron los hechos esto le dará un punto de partida al fabricante y la posible causa del error presentado.

Por otra parte el fabricante debe establecer un visor de sucesos, tanto el registro de aplicación como el registro del sistema contienen errores, advertencias y sucesos informativos relacionados con el funcionamiento de la tecnología TOUCH ID. Para identificar la causa de los problemas del flujo de mensajes, examine detenidamente los datos contenidos en el registro de aplicación y en el registro del sistema.

SOLUCION PROPUESTA.

Para proteger el sistema de este tipo de ataques el fabricante debe proteger la base de datos donde se almacenaran los puntos de cresta y valles de la huella dactilar y debe utilizar un buen algoritmo de seguridad para que al atacante le sea más difícil la intrusión al sistema.

o). RESTRICCION DE INSTALACION DE SOFTWARE

CONTROL 1. El fabricante debe establecer y aplicar reglas que rijan la instalación de software por parte de los usuarios.

En este fabricante debe desarrollar e implementar un procedimiento en el que alerte al usuario si al momento de instalar otras aplicaciones requiera la utilización de TOUCH ID dar al usuario la libertad si da permiso o no de utilizarlas con otras aplicaciones.

Para lograr que el control tenga éxito se debe realizar un método para poder analizar la vulnerabilidad de este control esto con el fin de tomar acciones correctivas y mitigar el riesgo al que se encuentre expuesto.

METODO PROPUESTO

El fabricante deberá realizar un desarrollo donde envié mensajes de alerta al momento de que otra aplicación requiera permisos para acceder al TOUCH ID.

Realizar pruebas donde se evidencien estas alertas documentar estas pruebas y establecer una directiva de que aplicaciones más comunes y pueden ser maliciosas para el sistema.

SOLUCION PROPUESTA.

Para proteger el sistema de este tipo de ataques el fabricante debe establecer reglas o directivas restrictivas de software malicioso que pueda instalarse en el sistema sin permiso del usuario establecer y configurar niveles de seguridad para evitar accesos mediante aplicaciones no autorizadas.

p). NOTIFICACION DE PUNTOS DEBILES DE LA SEGURIDAD

CONTROL 1. Todos los empleados, contratistas, terceras partes usuarias de los sistemas y servicios de información ofrecida por el fabricante debe ser obligados a anotar y notificar cualquier punto débil que observen o que sospechen que exista, en los sistemas o servicios.

En este fabricante debe desarrollar e implementar un procedimiento en el que alerte al usuario y envié los errores o fallos presentados cuando utilice el TOUCH ID con esto el fabricante podrá dar solución y corregir el problema.

Para lograr que el control tenga éxito se debe realizar un método para poder analizar la vulnerabilidad de este control esto con el fin de tomar acciones correctivas y mitigar el riesgo al que se encuentre expuesto.

METODO PROPUESTO

El fabricante deberá realizar un desarrollo donde envié mensajes de alerta al momento de que otra aplicación requiera permisos para acceder al TOUCH ID.

Realizar pruebas donde se evidencien estas alertas documentar estas pruebas y establecer una directiva de que aplicaciones más comunes y pueden ser maliciosas para el sistema.

SOLUCION PROPUESTA.

Para proteger el sistema de este tipo de ataques el fabricante deberá contar con un repositorio o centro de notificaciones donde se almacenen las notificaciones enviadas por el usuario debido a fallas en el TOUCH ID analizar que produjo el error si fue debido algún ataque y darles solución y respuesta con ello el fabricante mejorara esta tecnología.

q). VERIFICACION, REVISION Y EVALUACION DE LA CONTINUADAD DE LA SEGURIDAD DE LA INFORMACION

CONTROL 1. El fabricante debe comprobar los controles establecidos e implementados a intervalos regulares para asegurar que son válidos y eficaces durante situaciones adversas.

En este fabricante debe desarrollar e implementar un procedimiento el cual permita evaluar el nivel de seguridad de los componentes que conforman la tecnología TOCUH ID.

Para lograr que el control tenga éxito se debe realizar un método para poder analizar la vulnerabilidad de este control esto con el fin de tomar acciones correctivas y mitigar el riesgo al que se encuentre expuesto.

METODO PROPUESTO

El fabricante deberá mediante ataques al sensor puede ser mediante ecografías las cuales se puede obtener información acerca de las capas internas de la piel o incluso del flujo sanguíneo y así poder falsificar una huella e intentar acceder al sistema para determinar la vulnerabilidad de cada uno de los elementos que conformar el TOUCH ID. El fabricante debe estar continuamente evaluando y realizando auditorías internas y externas para así obtener resultados y mirar las

vulnerabilidades a la que se encuentra expuesto esta tecnología y que los riesgos se encuentran controlados.

SOLUCION PROPUESTA.

El fabricante deberá mediante listas de verificación o check list establecidos previamente por el fabricante realizar una auditoría de la tecnología TOUCH ID para obtener resultados graficarlos y saber en qué parte o en que elementos que conforman esta tecnología está siendo vulnerable a posibles ataques.

r). PROTECCION Y PRIVACIDAD DE LA INFORMACION DE CARÁCTER PERSONAL

CONTROL 1. El fabricante debe garantizarse la protección y la privacidad de los datos, según se requiera en la legislación y la reglamentación aplicables.

En este control el fabricante debe implementar un procedimiento donde asegure la protección y la privacidad de los datos del usuario según la norma LOPD (Ley orgánica de protección de datos de carácter personal). que tiene por objeto garantizar y proteger, en lo que concierne cavo al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor, intimidad y privacidad personal y familiar.

METODO PROPUESTO

El fabricante deberá realizar un ataques de SQL injection para así determinar que tal vulnerable es la base de datos que contienen las plantillas de los puntos de nuestras huellas digitales ya que si algún ataque prospera el fabricante debe utilizar algoritmos de encriptación por cada punto así le será más difícil acceder al atacante, el fabricante debe realizar pruebas y documentar el proceso mediante el cual se demuestre que es seguro.

SOLUCION PROPUESTA.

Para proteger el sistema de este tipo de ataques el fabricante deberá implementar algoritmos de encriptación de la información para que cuando prospere algún ataque la información se encuentre protegida.

5. CONCLUCIONES Y TRABAJO FUTURO.

En el presente proyecto se han estudiado las vulnerabilidades que presentan los sistemas basados en reconocimiento biométrico de huella dactilar. En concreto, se han detallado los diferentes tipos de ataques a los que está expuesto TOUCH ID y observamos como los atacantes han logrado evadir esta seguridad dejando en evidencia que este sistema no es seguro aun así realizando experimentos en público como las investigaciones en el **Instituto Nacional de Informática de Japón** han desarrollado un **'método que permite copiar las huellas dactilares de fotografías hasta a tres metros de distancia por una cámara digital'.** (e-volución, 2017)**,** la cual a partir de una selfie puede falsificar una huella digital.

También lo demuestra **Universidad de New York y Michigan State**, se podría burlar el sistema, en un 65% de los casos, por medio de "huellas maestras" creadas de manera artificial. (INFOBAE, 2017), en fin existen infinitas posibilidades de ataques que se encuentran surgiendo en el día a día para demostrar que no es tan seguro esta tecnología TOUCH ID.

A raíz de todas estas investigaciones y las que se han expuesto en este proyecto es importante que la tecnología TOUCH ID alrededor de sus elementos que la componen implementen políticas y controles de seguridad siempre basados en las normas de la familia ISO/IEC 27000 ya con esto puede que se garantice la seguridad de la información al usuario final.

El hecho de que los ataques **Hill Climbing** requieran un número mayor de iteraciones que un ataque de fuerza bruta, no debe ser realmente interpretado como un indicador absoluto de que son menos eficaces que los ataques de fuerza bruta. Para llevar a cabo un ataque de fuerza bruta es necesario una base de

datos de huellas que tenga un número mayor de muestras a las necesarias, en este caso, alrededor de 2000. En cambio, para realizar un ataque **Hill Climbing** no es necesario disponer de huellas reales de muestra y únicamente será necesario implementar el algoritmo adaptado al sistema. Además, se ha observado que, en un número de iteraciones superior al establecido, en todos los casos del mismo orden de magnitud, se logra llevar a la mayoría de los ataques con éxito.

Como trabajo futuro se propone en primer lugar la optimización de los algoritmos de ataque que se mostraron en el proyecto con el fin de que requieran un menor número de iteraciones en promedio.

Se propone además el estudio de la vulnerabilidad de sistemas multimodales frente a ataques Hill Climbing. Es posible combinar los ataques ya existentes en la literatura ante sistemas de reconocimiento de huella dactilar para lograr más resultados y poner la alerta a los fabricantes de que estos sistemas pueden ser vulnerados y deben centrar sus esfuerzos a que este sistema sea seguro.

En general pueden estudiarse y clasificarse nuevas vías de ataque, tanto directo como indirecto, a sistemas de reconocimiento biométrico basados en otros identificadores diferentes a la huella.

Continuando con el trabajo realizado en este proyecto y dada la relevancia que han cobrado los sistemas basados TOUCH ID se propone el análisis exhaustivo de sus vulnerabilidades a nivel software, debido a la escasez de recursos por parte de estos sistemas obliga a simplificar los algoritmos del comparador, por lo que a priori pueden ser más vulnerables.

Los controles de seguridad según la ISO/IEC 27001:2013 obtenidos en el presente proyecto se han empleado para que el fabrícate tenga los tenga en cuenta en los desarrollos DE TOUCH ID es factible que los pueda mejorar e implementar nuevos métodos de vulnerabilidades si así lo requiera, pero es el punto de partida para un análisis más detallo con respecto al seguridad de TOUHC ID.

Pueden estudiarse las vulnerabilidades de los sistemas de reconocimiento de huella dactilar en función de la calidad de la huella y del tipo del sensor utilizado. Es probable que la robustez de los sistemas sea dependiente de la calidad de las imágenes, dado que su rendimiento es, como ya se ha mencionado en el proyecto, muy dependiente de ella [Alonso-Fernández et al., 2005].

Se propone también el estudio de ataques de fuerza bruta basados en la generación de imágenes sintéticas de huella dactilar. En la actualidad existe software que lo realiza, como SFINGE (Synthetic Fingerprint Generator) (D. Maltoni, 2003), y puede permitir realizar ataques que, al igual que en el caso de Hill Climbing, no requieran imágenes reales de huella dactilar.

Parte del trabajo realizado en este proyecto, además de los controles de seguridad establecido con sus métodos y sus posibles soluciones han sido recogidos y publicados por varios autores ya mencionados los cuales han aportado estudios procedimientos y resultados con base a la seguridad de los sistemas biométricos.

Bibliografía

A.K. Jain, .. P. (2000). Filterbank-Based Fingerprint Matching. . En *IEEE Transactions on Image Processing* (págs. 9:846-859).

A.K. Jain, A. R. (2004). Circuits Systems for Video Technology,. En *IEEE Trans.An introduction to biometric recognition.* (págs. 14(1):4-20,).

D. Maltoni, D. M. (2003). *Handbook of Fingerprint Recognition.* Springer .

Galbally-Herrero. (2006).

IBERLEY. (27 de 11 de 2017). *IBERLEY COLEX.* Obtenido de IBERLEY COLEX: https://www.iberley.es/legislacion/reglamento-ue-2016-679-27-abr-doue-reglamento-general-europeo-proteccion-datos-gdpr-rgpd-24473701

J. Galbally-Herrero, J. F.-A.-G.-F.-G. (October 2006). *On the vulnerability of fingerprint verification sys-tems to fake fingerprint attacks, to appear.* USA: IEEE Intl. Carnahan Conf. on Security Technology, ICCST, IEEE Press, Lexington.

J. Keuning., T. v. (2000). Biometrical Fingerprint Recognition Don't Get Your Fin-gers Burned. Proceedings of: IFIP TC8/WG8.8 Fourth Working Conference on Smart Card Research and Advanced Applications. En *Biometrical Fingerprint Recognition Don't Get Your Fin-gers Burned. Proceedings of: IFIP TC8/WG8.8 Fourth Working Conference on Smart Card Research and Advanced Applications* (págs. 289-303). Kluwer Academic Publishers.

Kàkona, M. (2001). *http://home.i.cz/kakl/biometrics/Biometricsyesorno.htm*. Obtenido de http://home.i.cz/kakl/biometrics/Biometricsyesorno.htm: http://home.i.cz/kakl/biometrics/Biometricsyesorno.htm

L. Thalheim, J. K. (11/2002). Body Check: Biometric Access Protection De-vices and their Programs Put to the Test. *C't Magazin für Computertechnik*, 114.

Limor Kessem, I. (2017). *IBM Security: Future of Identity Study Consumer perspectives on authentication.* IBM SECURYTY.

Mañas, J. L. (2016). REGLAMENTO GENERAL DE PROTECCION DE DATOS. En J. L. Mañas, *REGLAMENTO GENERAL DE PROTECCION DE DATOS* (pág. 862). MADRID: REUS.

Soutar., C. (2002). *Biometric System performance and security.* Obtenido de Biometric System performance and security: http://www.bioscrypt.com/assets/bio_paper.pdf

T. Matsumoto, H. M. (2002). *Impact of Artificial Gummy Fingers on Fingerprint Systems. Proceedings of SPIE Vol. #4677,, Optical Security and Counterfeit Deterrence Techniques IV.* SPIE.

U. Uludag, A. J. (January 2004.). *Attacks on Biometric Systems: A Case Study in Fingerprints,Security, Steganography and Watermarking of Multimedia Con-tents VI, 5306:622-633, .* San Jose, CA: SPIE-EI .

UMANICK. (14 de 10 de 2013). *UMANICK*. Obtenido de UMANICK: http://www.umanick.com/la-huella-dactilar-a-fondo-tipos-de-escaneres-parte-iii/

UNIVERSIDAD INTERNACIONAL DE LA RIOJA

MAESTRIA EN SEGURIDAD INFORMATICA

ESTUIDIANTE: ANDRES PALACIOS ORTEGA

2018.

ANEXO 1

TABLA DE EVALUACION MATRIZ DE RIESGO ANEXO 1

Los criterios de evaluación definidos para cada una de los controles que se indicaron en la matriz en Excel anexa a este documento se desarrollan de la siguiente manera:

EJEMPLO:

CRITERIOS DE EVALUACION

- Establecer
- Documentar
- Revisar

Esto significa:

- Si la política cumple con los 3 (tres) criterios tendrá una probabilidad de ocurrencia.

ISO/IEC 27001:2013				METODOS		CHECKLIST	PROBALIDAD DE OCURRENCIA E IMPACTO SOBRE EL SISTEMA SI SE MATERIALIZA		
ITEM	DESCRIPCION	CONTROL	DESCRIPCION DEL RIESGO PARA TOUCH ID	METODO PARA ANALIZAR LA VULNERABILIDAD	CRITERIO	EVALUACION (1 Ò 0)	BAJO	MEDIO	ALTO
A.9.1.1	POLITICA DE CONTROL DE ACCESO	El fabricante debe establecer, documentar y revisar una política de control de acceso basada en los requisitos de negocio y de seguridad de la información.	R1.Cualquier persona podra acceder sin restricciones al sistema y corromperlo	El fabricante debe presentar la política de control de acceso para establecer y documentar el procedimiento de accecibilad a travez del sensor de huella. Ademas debe identificar los elementos de seguridad necesarios para que dicho sendor no este expuesto a posibles ataques.	ESTABLECER	1	X		
					DOCUMENTAR	1			
					REVISAR	1			

- Si cumple con solo 2(Dos) criterios la probabilidad de ocurrencia es Media

ISO/IEC 27001:2013				METODOS		CHECKLIST	PROBALIDAD DE OCURRENCIA E IMPACTO SOBRE EL SISTEMA SI SE MATERIALIZA		
ITEM	DESCRIPCION	CONTROL	DESCRIPCION DEL RIESGO PARA TOUCH ID	METODO PARA ANALIZAR LA VULNERABILIDAD	CRITERIO	EVALUACION (1 Ò 0)	BAJO	MEDIO	ALTO
A.9.1.1	POLITICA DE CONTROL DE ACCESO	El fabricante debe establecer, documentar y revisar una política de control de acceso basada en los requisitos de negocio y de seguridad de la información.	R1.Cualquier persona podra acceder sin restricciones al sistema y corromperlo	El fabricante debe presentar la política de control de acceso para establecer y documentar el procedimiento de accecibilad a travez del sensor de huella. Ademas debe identificar los elementos de seguridad necesarios para que dicho sendor no este expuesto a posibles ataques.	ESTABLECER	1			
					DOCUMENTAR	1			
					REVISAR	0		X	

- Si no cumple con ningún criterio la probabilidad de ocurrencia es alto.

ISO/IEC 27001:2013				METODOS		CHECKLIST	PROBALIDAD DE OCURRENCIA E IMPACTO SOBRE EL SISTEMA SI SE MATERIALIZA		
ITEM	DESCRIPCION	CONTROL	DESCRIPCION DEL RIESGO PARA TOUCH ID	METODO PARA ANALIZAR LA VULNERABILIDAD	CRITERIO	EVALUACION (1 Ò 0)	BAJO	MEDIO	ALTO
A.9.1.1	POLITICA DE CONTROL DE ACCESO	El fabricante debe establecer, documentar y revisar una política de control de acceso basada en los requisitos de negocio y de seguridad de la información.	R1.Cualquier persona podra acceder sin restricciones al sistema y corromperlo	El fabricante debe presentar la política de control de acceso para establecer y documentar el procedimiento de accecibilad a travez del sensor de huella. Ademas debe identificar los elementos de seguridad necesarios para que dicho sendor no este expuesto a posibles ataques.	ESTABLECER	0			X
					DOCUMENTAR	0			
					REVISAR	0			

De tal forma que para dicha matriz se pueden incluir nuevos controles que nos permitan evaluar el riesgo para esta tecnología.

ISO/IEC 27001:2013				METODOS	CRITERIO DE EVALUACION	CHECKLIST	PROBALIDAD DE OCURRENCIA E IMPACTO SOBRE EL SISTEMA SI SE MATERIALIZA			SOLUCIONES PROPUESTA
ITEM	DESCRIPCION	CONTROL	DESCRIPCION DEL RIESGO PARA TOUCH ID	METODO PARA ANALIZAR LA VULNERABILIDAD	CRITERIO	EVALUACION (1 Ò 0)	BAJO	MEDIO	ALTO	SOLUCION
A.9.1.1	POLITICA DE CONTROL DE ACCESO	El fabricante debe establecer, documentar y revisar una política de control de acceso basada en los requisitos de negocio y de seguridad de la información.	R1.Cualquier persona podra acceder sin restricciones al sistema y corromperlo	El fabricante debe presentar la politica de control de acceso para establecer y documentar el procedimiento de accecibilad a travez del sensor de huella. Ademas debe identificar los elementos de seguridad necesasrios para que dicho sendor no este expuesto a posibles ataques.	ESTABLECER DOCUMENTAR REVISAR	0 0 0			X	para proteger un sistema de esta clase de ataques sería la de que el matcher no revelase la puntuación sino simplemente la indicación de aceptación o rechazo por parte del sistema. Esta solución es viable en ciertos casos, como en algunos sistemas embebidos, pero para los que em-pleen varios rasgos biométricos (sistemas multimodales), la puntuación debe ser conocida por otros elementos del sistema y por lo tanto puede ser visible.
A.9.1.2	ACCESO A LAS REDES A LOS SERVICIOS DE RED	El fabricante debe proporcionar a los usuarios el acceso a las redes y a los servicios en red para cuyo uso hayan sido específicamente autorizados.	R2.acceso a la red para descarga de malware en el sistema o de apllicaciones para corromper el sistema	El fabricante puede medir la transluminancia del dedo, detectando la luz que atraviesa el dedo o la reflexión de la luz en el dedo mediante un emisor y un receptor luminoso. Mediante una fotopletismografía se puede medir el pulso cardiaco a través de la detección de la variación del volumen de sangre que circula por el dedo asi poder acceder al sistema, documentar y sacar concluciones	PERMISOS DE RED DOCUMENTAR REVISAR ACCESOS DE RED	0 0 0			X	Se propone esta solución para proteger al sistema de huellas falsificadas por eso es importe que el sensor este en el ranking de los mejores en el mercado que permita conexiones a redes de Wifi seguras y así brindar una comunicación más segura con el usuario.
A.9.2.1	REGISTRO Y BAJA DE USUARIO	El fabricante debe implementar un procedimiento formal de registro y retirada de usuarios que haga posible la asignación de los derechos de acceso.	R3.acceso a los registros se usuarios que existan en la base de datos	El fabricante puede ser interceptar el canal y se puede introducir otra información que sustituya a la enviada por el sensor.	IMPLEMENTAR PROCEDIMIENTO REGISTRO DE BAJA RETIRADA DE USUARIOS	0 0 0			X	Para protegernos de este ataque es conveniente que el canal de couminicacion eset muy bien protegido con algun algoritmo de ecriptacion
A.9.2.2	PROVISION DE ACCESO DE USUARIO	El fabricante debe implementar un procedimiento formal para asignar o revocar los derechos de acceso para todos los tipos de usuarios de todos los sistemas y servicios.	R4.Suplantacion de credenciales de acceso.	El fabricante con coperacion del usuario se obtiene de una huella latente de un usuario en un vaso de vidrio. En primer lugar se espolvoreó con un fino polvo coloreado para posteriormente levantarla por medio de cinta adhesiva. A continuación tomaron una fotografía de la huella (con una cámara analógica convencional) y situaron el nega-tivo sobre una placa de prototipado PCB (Printed Circuit Board). Después de exponer la placa con el negativo encima a rayos ultra violeta y someterla a un baño de ácido la huella queda perfectamente marcada sobre la superficie de la misma. A partir de la huella de la PCB y empleando de nuevo silicona líquida se pudo obtener una réplica de la huella	IMPLEMENTAR PROCEDIMIENTO REVACION DE DERECHOS DE ACCESO LISTADO DE TIPOS DE USUARIOS DEL SISTEMA	0 0 0			X	Para proteger el sistema de este tipo de ataques el fabricante debe proporcionar que los sensores de huella so sean suplantados y dar recomendaciones al usuario para que este se mas precavido de donde deja sus huellas dactilares ya que ingenuamente puede ser víctima de un ataque.
A.9.2.3	GESTION DE PRIVILEGIOS DE ACCESO	La asignación y el uso de privilegios de acceso debe estar restringida y controlada poe el fabricante.	R5.Ataque de denegacion de servicios del sistema	El fabricante debe realizar el ataque directamente a la base de datos del sistema de reconocimiento biométrico. En él, utilizando un comparador de huella comercial, se realiza ingeniería inversa sobre el patrón de datos de las minucias y se generan las imágenes artificiales correspondientes a las huellas dactilares interceptadas. En este tipo de ataques estarían además contemplados los casos en los que el atacante tuviera acceso privilegiado a la base de datos o al canal de comunicación entre el comparador y la base de datos. En ese caso sería necesario que conociese el formato concreto en que se almacenan los patrones en la misma, y los modificase introduciendo nuevos patrones, cambiando o eliminando alguno ya existente.	ASIGNACION DE PRIVILEGIOS EN EL SISTEMA LISTA DE ROLES Y PERFILES DE USUARIOS REGISTRO DE USUARIOS	0 0 0			X	Para proteger el sistema de este tipo de ataques es necesario que el fabricante tenga un buen conocimiento en el formato concreto en que se almacenan los patrones en la base de datos y los pueda modificar introduciendo nuevos patrones, cambiando o eliminando alguno ya existente para que los patrones que se almacenen en la base de datos sean mas seguros.
A.9.2.4	GESTION DE LA INFORMACION SECRETA DE AUTENTICACION DE USUARIOS	La asignación de la información secreta de autenticación debe ser controlada a través de un proceso formal de gestión definida por el fabricante.	R6.Corrupción o modificación de la información.	El fabricante debe utlizar la huella que se realza con polvo de grafito para después obtener a partir de ella una imagen digital e imprimirla en papel de transparencia con una impresora láser, cuyo toner genera un pequeño relieve. A continuación se cubre con cola para madera y se espera a que seque para posteriormente despegarla de la hoja. La falsificación queda así completa.	PRODECIMIENTO PARA INFORMACION SECRETA REVISION ACTUALIZACION PROCEDIMIENTO	0 0 0			X	Para proteger el sistema de este tipo de ataques el fabricante debe adoptar un scanner que permita realizar un doble factor de autenticación que si se logra acceder mediante una huella falsificada obligue a la autenticación con otro método de autenticación por ejemplo con el iris y una contraseña alfanumérica etc.
A.9.2.5	REVISION DE LOS DERECHOS DE ACCESO DE USUARIO	Los propietarios de los activos deben revisar los derechos de acceso de usuario definidos por el fabricante a intervalos regulares.	R7.interrupcion de servicios	En este método el fabricante debe centrarse directamente a la extracción de características para ello debe utilizar un algoritmo seguro y realizar pruebas mediante las técnicas de comparación, como por ejemplo la de minucias o basadas en alineamiento de patrones y así poder determinar qué tan difícil es para al atacante acceder al sistema.	REVISION DERECHOS DE ACCESO ACTUALIZACION DERECHOS DE ACCESO	0 0 0			X	Para proteger el sistema de este tipo de ataques el fabricante debe tener un buen algoritmo de encriptación, como se ha mencionado anteriormente está en la base fundamental para que un atacante le sea más difícil acceder al sistema es por ello que el fabricante no debe reducir costos al momento de implantar una tecnología como esta en donde la información es el actor principiar de esta cadena.
A.9.4.1	RESTRICCION DEL ACCESO DE LA INFORMACION	El fabricante debe restringir el acceso a la información y a las funciones de las aplicaciones, de acuerdo con la política de control de acceso definida.	R8.Acceso no autorizado a informacion sencible	el fabricante debera basarse en tecnicas basadas en correlacion este metodo sirve para hacer el calculo de correlacion entre la imagen de muestra y la de entrada tratando de maximizarla Cuanto mayor sea la correlación mayor será la similitud entre las huellas a comparar y su maximización permitirá calcular el valor del desplazamiento y la rotación que hacen que las dos imágenes sean lo más parecidas posibles.	RESTICCIONES FUNCIONES Y APLICACIONES POLITCA DE CONTROL	0 0 0			X	Para proteger el sistema de este tipo de ataques el fabricante debe implementar un sistema detector de intrusos que ponga alerta el sistema y no permita que a través de imágenes puedan acceder a nuestro sistema.
A.9.4.2	PROCEDIMIENTOS SEGUROS DE INCIO DE SESION	Cuando así se requiera en la política de control de acceso, el acceso a los sistemas y a las aplicaciones se debe controlar por medio de un procedimiento seguro de inicio de sesión definido por el fabricante.	R9.acceso al sistema por un atacante si no se tiene un control de acceso al sistema	El fabricante debera basarse en técnicas basadas en minucias son los más conocidos y de uso más extendido en la actualidad. Están basados directamente en la forma en que los expertos forenses realizan la comparación entre huellas. en este caso la representación es un vector de características de longitud variable cuyos elementos son las minucias de la huella. Cada minucia se puede describir a partir de un número de atributos como su posición en la imagen, su orientación, tipo (final de cresta o bifurcación de cresta), un peso basado en la calidad de la imagen en su vecindad, etc. La mayor parte de los algoritmos basados en minucias consideran cada singularidad como una tupla (,,)xyθ indicando la posición horizontal y vertical de la minucia y su orientación en la imagen.	POLITICA DE CONTROL DE ACCESO PROCEDIMIENTO SEGURIO REVISION	0 0 0			X	Para proteger el sistema de este tipo de ataques el fabricante debe implementar un sistema donde aparte de la autenticación por TOCUH ID debe tener un factor doble de autenticacion en nuestro sistema.
A.9.4.3	SISTEMA DE GESTION DE CONTRASEÑAS	Los sistemas para la gestión de contraseñas deben ser interactivos y establecer contraseñas seguras y robustas definidas por el fabricante.	R10.acceso al sistema por un atacante	Técnicas basadas en patrones de crestas o texturas se describe una técnica basada en texturas locales en la que el área de la huella se subdivide en zonas con respecto al núcleo de la huella. Se calcula un vector de características basado en la información de cada zona resultante de la subdivisión.	GESTION DE CONTRASEÑAS INTERVALOS DE TIEMPOS POLITICA DE CONTRASEÑA	0 0 0			X	Para proteger el sistema de este tipo de ataques el fabricante debe implementar un sistema donde aparte de la autenticación por TOCUH ID debe proteger el sistema con un algoritmo de encriptación muy seguro para las puntuaciones y no sea tan fácil lograr descifrarlas.
A.9.4.4	USO DE UTILIDADES CON PRIVILEGIOS DEL SISTEMA	El fabricante debe restringir y controlar rigurosamente el uso de utilidades que puedan ser capaces de invalidar los controles del sistema y de la aplicación.	R11.acceso por medio de malware malicioso	son viables sólo si el atacante conoce alguna parte de la arquitectura del sistema de autenticación biométrica y/o tiene privilegios de acceso. Este hecho condiciona su facilidad de aplicación con respecto a los ataques al sensor. En cambio, no precisan crear modelos físicos de la huella sino que se deberá disponer de conocimientos acerca de la parte software del sistema.	RESTRICCIONES REVISION UTILIDADES DEL SISTEMA	0 0 0			X	Para proteger el sistema de este tipo de ataques el fabricante debe implementar un procedimiento el cual se defina que algoritmo puede ser el mejor para utilizar y realizar pruebas de intrusión para comenzar a evaluar que tan seguro es como todo sistema no se puede garantizar que sea 100% seguro pero si una alta dificultad de poder acceder al sistema.
A.9.4.5	CONTROL DE ACCESO AL CODIGO FUENTE DE LOS PROGRAMAS	El fabricante debe restringir el acceso al código fuente de los programas.	R12.acceso al codigo fuente para poder acceder y corromper el sistema	Metodo por el cual un programa puede suplantar al extractor de características a modo de troyano y enviar características generadas a voluntad del atacante al matcher.	CONTROL DE ACCESO REVISION RESTRICCIONES	0 0 0			X	el fabricante nunca debe permitir que el matcher revele la puntuación sino simplemente la indicación de aceptación o rechazo por parte del sistema. Esta solución es viable en ciertos casos, como en algunos sistemas embebidos, pero para los que empleen varios rasgos biométricos (sistemas multimodales), la puntuación debe ser conocida por otros elementos del sistema y por lo tanto puede ser visible.
A.10.1.1	POLITICA DE USO DE LOS CONTROLES CRIPTOGRAFICOS	El fabricante debe desarrollar e implementar una política sobre el uso de los controles criptográficos para proteger la información.	R13.cambios en el algoritmo de autenticacion	El fabricante deberá utilizar el método de ataque hill-climbing donde el objetivo principal es el de atacar directamente el matcher y no utiliza información alguna de la imagen de la huella. Emplea exclusivamente patrones sintéticos de minucias generados aleatoriamente o según una distribución que se estime aproximada a la huella, basada en histogramas de minucias de las huellas de una base de datos. Únicamente es necesario conocer cuál es el sensor, para así saber cuál es su resolución y el tamaño de las imágenes que genera.	ALGORITMOS CRIPTOGRAFICOS POLITICA DE USO REVISION	0 0 0			X	para protegernos de este ataque en En [Soutar, 2004] se propone cuantificar las puntuaciones devueltas por el matcher co-mo una método de protección ante ataques hill-climbing. La ventaja de esta medida es clara, puesto que al basarse el ataque en pequeñas modificaciones de la plantilla inicial, una leve mejora o un leve empeoramiento no podrán, en general, ser detectados al per-manecer la mejoría dentro del mismo paso de cuantificación y mantenerse por lo tanto invariable la puntuación de salida.
A.10.1.2	GESTION DE CLAVES	El fabricanrte debe desarrollar e implementar una política de sobre el uso, la protección y la duración de las claves de cifrado a lo largo de todo su ciclo de vida.	R14.cambios de claves con las que exiten a travez del extrator de caracteristicas y la base de datos	El fabricante deberá utilizar un método en el cual le permita reactivar la huella de un usuario anterior y en un sensor capacitivo empleando el aliento, utilizando una cinta adhesiva con polvo de grafito o presionando con una bolsa de plástico fina llena de agua y apoyándose también junto con las técnicas descritas anteriormente (minucias, patrones de crestas o texturas etc.) intentar lograr acceder al sistema.	POLITICA DE USO DE CLAVES ALGORITMO DE CIFRADOS REVISION	0 0 0			X	Para proteger el sistema de este tipo de ataques el fabricante mediante la política de gestión de claves debe obligar al usuario cambiar sus claves de acceso periódicamente, por ejemplo ir utilizando cada una de las huellas de sus dedos con esto podrá minimizar posibles ataques.
A.12.2.1	CONTROLES CONTRA EL CODIGO MALICIOSO	El fabricante debe implementar los controles de detección, prevención y recuperación que sirvan como protección contra el código malicioso, así como procedimientos adecuados de concienciación al usuario.	R15.ataques de codigo malicioso a traves de aplicaciones o programas que alteren el sistema	Metodo en ecual mediante un programa puede suplantar a modo de troyano al matcher y enviar una puntuación falsa o una decisión sí/no a la aplicación de autenticación.	CONTROLES DE DETECCION CONTROLES DE PREVENCION CONTROLES DE RECUPERACION	0 0 0			X	Para proteger el sistema de este tipo de ataques el fabricante no debe utilizar sensores baja calidad ya que esto puede ocasionar muchos fallos de seguridad al usuario todo lo contrario debe utilizar lo último en tecnología para poder ofrecer al usuario ese plus adicional en el producto de que puede estar tranquilo y que es muy difícil que un atacante pueda acceder a su información personal. Es importante que el fabricante mantenga al usuario actualizado y concientizarlo de utilizar los procedimientos adecuados definidos previamente en la tecnología TOCUH ID y se ciña a lo estipulado por el fabricante.
A.12.4.1	REGISTRO DE EVENTOS	El fabricante debe registrar, proteger y revisar periódicamente las actividades de los usuarios, excepciones, fallos y eventos de seguridad de la información.	R16.accesos desconocidos por el uaurio	El fabricante deberá crear una base de datos y establecer los periodos de tiempo en que registraran los log del sistema contra fallos o posibles ataques con el fin de saber la fecha y la hora en que ocurrieron los hechos esto le dará un punto de partida al fabricante y la posible causa del error presentado. Por otra parte el fabricante debe establecer un visor de sucesos, tanto el registro de aplicación como el registro del sistema contienen errores, advertencias y sucesos informativos relacionados con el funcionamiento de la tecnología TOUCH ID. Para identificar la causa de los problemas del flujo de mensajes, examine detenidamente los datos contenidos en el registro de aplicación y en el registro del sistema	REGISTRO DE EVENTOS REVISION PROTECCION	0 0 0			X	Para proteger el sistema de este tipo de ataques el fabricante debe proteger la base de datos donde se almacenaran los puntos de cresta y valles de la huella y debe utilizar un buen algoritmo de seguridad para que al atacante le sea más difícil la intrusión al sistema.
A.12.6.2	RESTRICCION DE INSTALACION DE SOFTWARE	El fabricante debe establecer documentar y aplicar reglas que rijan la instalación de software por parte de los usuarios.	R17.Instalacion de software malintencionado	El fabricante deberá realizar un desarrollo donde envié mensajes de alerta al momento de que otra aplicación requiera permisos para acceder al TOUCH ID. Realizar pruebas donde se evidencien estas alertas documentar estas pruebas y establecer una directiva de que aplicaciones pueden ser maliciosas para el sistema.	ESTABELCIMIENTO DE REGLAS DOCUMENTAR REVISION	0 0 0			X	Para proteger el sistema de este tipo de ataques el fabricante debe establecer reglas o directivas restrictivas de software malicioso que pueda instalarse en el sistema sin permiso del usuario establecer y configurar niveles de seguridad para evitar accesos mediante aplicaciones no autorizadas.
A.16.1.3	NOTIFICACION DE PUNTOS DEBILES DE LA SEGURIDAD	Todos los empleados, contratistas, terceras partes usuarias de los sistemas y servicios de información ofrecida por el fabricante debe ser obligados a anotar y notificar cualquier punto débil que observen o que sospechen que exista, en los sistemas o servicios.	R18.acceso a travez de huecos de seguridad tanto fisica commo a nivel de codigo	Para proteger el sistema de este tipo de ataques el fabricante deberá contar con un repositorio o centro de notificaciones donde se almacenen las notificaciones enviadas por el usuario debido a fallas en el TOUCH ID analizar que produjo el error si fue debido algún ataque y darles solución y respuesta con ello el fabricante mejorara esta tecnología.	BITACORA DE HALLAZGOS DOCUMENTAR REVISAR	0 0 0			X	Para protgernos de este ataque se recomienda tener todos los parches y/o actualuizaciones del sistema para prevenir un acceso no autorizados por errores del sistema que dejen puertas traseras abiertas a los atacantes.
A.17.1.3	VERIFICACION, REVISION Y EVALUACION DE LA CONTINUADAD DE LA SEGURIDAD DE LA INFORMACION	El fabricante debe comprobar los controles establecidos e implementados a intervalos regulares para asegurar que son válidos y eficaces durante situaciones adversas.	R19.acceso de atacantes a travez de falsificaciones de huella	El fabricante deberá mediante ataques al sensor puede ser mediante ecografías las cuales se puede obtener información acerca de las capas internas de la piel o incluso del flujo sanguíneo y así poder falsificar una huella e intentar acceder al sistema para determinar la vulnerabilidad de cada uno de los elementos que conformar el TOUCH ID. Este método es poco viable ya que su automatización es compleja y suele requerir un post-análisis por parte de un experto pero si el fabricante quiere ofrecer seguridad no debería descartar este método.	CONTROLES ESTABLECIDOS COMPROBACION DE CONTROLES ASEGURAMIENTO DE CONTROLES	0 0 0			X	El fabricante deberá mediante listas de verificación o check list establecidos previamente por el fabricante realizar una auditoría de la tecnología TOUCH ID para obtener resultados graficarlos y saber en qué parte o en que elementos que conforman esta tecnología está siendo vulnerable a posibles ataques.
A.18.1.4	PROTECCION Y PRIVACIDAD DE LA INFORMACION DE CARÁCTER PERSONAL	El fabricante debe garantizar la protección y la privacidad de los datos, según se requiera en la legislación y la reglamentación aplicables.	R20.Perdida de informacion	El fabricante deberá realizar un ataques de SQL injection para así determinar que tal vulnerable es la base de datos que contienen las plantillas de los puntos de nuestras huellas digitales ya que si algún ataque prospera el fabricante debe utilizar algoritmos de encriptación por cada punto así le será más difícil acceder al atacante, el fabricante debe realizar pruebas y documentar el proceso mediante el cual se demuestre que es seguro.	PROTECCION PRIVACIDAD REVISAR	0 0 0			X	Para proteger el sistema de este tipo de ataques el fabricante deberá implementar algoritmos de encriptación de la información para que cuando prospere algún ataque la información se encuentre protegida.