La seguridad de mañana: Estado del arte sobre la Seguridad en los Dispositivos Médicos Implantables

Carmen Cámara
Depto. de Informática
Universidad Carlos III de Madrid
Email: mariacarmen.camara@alumnos.uc3m.es

Pedro Peris-Lopez
Depto. de Informática
Universidad Carlos III de Madrid
Email: pperis@inf.uc3m.es

Benjamín Ramos
Depto. de Informática
Universidad Carlos III de Madrid
Email: benja1@inf.uc3m.es

***Resumen*—El campo de la bioingeniería se encuentra actualmente en expansión. De éste nacen nuevas tecnologías orientadas a un tratamiento más eficiente de diversas patologías o deficiencias humanas. Un ejemplo de ello son los dispositivos médicos implantables (IMDs), artefactos que cada vez albergan más capacidad de computo, decisión y comunicación. Diversos trabajos en el campo de la seguridad han identificado riesgos de seguridad y privacidad en estos dispositivos, que podrían tener consecuencias fatales para el paciente. Este artículo resume los principales objetivos de seguridad que los dispositivos del futuro deberían contemplar, las tensiones que surgen entre estos objetivos y los principales trabajos orientados a dotar de la seguridad y privacidad necesaria a los IMDs.**

Palabras clave: IMD, comunicación wireless, telemetría, seguridad, privacidad, control de acceso, tensiones, vulnerabilidades.

Terminología:
IMD: Dispositivo Médico Implantable (Implantable Medical Device, IMD). Dispositivo implantado en el cuerpo humano, que puede comunicarse via wireless con otros dispositivos.
DAI: Desfibrilador Automático Implantable.
Lector: Dispositivo capaz de interactuar con el IMD mediante comunicación wireless.
Programador: Lector/persona con permisos (o que debería contar con ellos) para establecer comunicación con el IMD (ej., el personal médico).
IBN: Intra Body Network, conjunto de IMDs funcionando en un solo paciente. En la mayoría de los casos se tratará de uno sólo, pero pudieran ser más funcionando en colaboración.
FCC: U.S. Federal Communications Commission.
FDA: Food and Drug Administration: Agencia de Medicamentos o Alimentos; perteneciente al ministerio de Salud y Servicios Humanos de EEUU.
EMA: European Medicines Agency, Agencia Europea de Medicamentos.

I. Introducción

I-A. Qué es un IMD

Se define como *IMD* todo dispositivo permanente o semipermanente implantado en un paciente, cuya función puede ser el tratamiento de patologías, la mejora en el funcionamiento de alguna parte del cuerpo humano, o el desarrollado de funcionalidad o habilidad que antes no se tenía [1].

Un *IMD* puede ser cualquier dispositivo implantado en el cuerpo humano, ya sea un marcapasos, un *DAI* [2], un sistema de administración de medicación, un neuroestimulador [3], etc.

Estos dispositivos son cada vez más utilizados para tratar, de manera más eficiente, que los métodos tradicionales, una serie de dolencias como arritmias [4], diabetes, parkinson, alzheimer, depresión, etc. Son implantados 2-3 cm debajo de la piel y se conectan con el órgano que necesite tratamiento y/o monitorización.

I-B. Telemetría

Los nuevos diseños de *IMDs* basan una parte de su funcionalidad en la comunicación a distancia con un *lector* para realizar tareas de diagnostico o terapia. El uso de telemetría incluye la medición y registro de parámetros fisiológicos del paciente, que son los que se enviarán vía wireless al personal médico. El uso de esta tecnología está aceptado por la *FCC* [5].

Para que esta comunicación a distancia sea posible, los implantes incorporan receptores y transmisores wireless, que permiten al *IMD* comunicarse con un *lector*/*programador*, lo cual permite monitorear el dispositivo e incluso actualizarlo de manera remota. Las ventajas que esto incluye son: 1) El seguimiento puntual de los parámetros fisiológicos del paciente y demás sintomatología registrada por el mismo; 2) Un mayor grado de vigilancia en el funcionamiento del implante; y 3) La reducción del tiempo en el seguimiento del paciente por parte del personal médico y del tiempo empleado por el propio paciente, que con la transmisión electrónica de datos, no tendrá que acudir al centro de salud.

I-C. Por qué se necesitan medidas de seguridad

La comunicación a distancia expone al *IMD* a entornos abiertos que no se habían considerado anteriormente, haciendo que sea posible una intercepción de la comunicación y el ataque al dispositivo [6]. Esto introduce metas de seguridad nuevas en el campo, ya que un ataque de seguridad a estos dispositivos puede comprometer la integridad física del paciente que lo porta [7] y las consecuencias derivadas pueden ser fatales [8]. Este hecho está reconocido por la *FDA* [9]. Además se sabe que hoy día implantes como *DAIs*, que carecen de mecanismos de autenticación, siguen siendo utilizados [10].

Si existen vulnerabilidades en la comunicación entre el *IMD* y el *programador*, un adversario podría monitorear y alterar las funciones del implante, sin necesidad de encontrarse físicamente cerca de la víctima [5]. Por otro lado, el *IMD* almacena datos muy sensibles del paciente (como señales vitales, terapia, diagnóstico y datos personales como fecha de nacimiento, nombre u otro tipo de identificadores) de manera que es un requisito imprescindible asegurar la seguridad y la privacidad del *IMD*. De lo contrario estos datos podrían ser conocidos mediante escucha del canal. Además, hoy en día contar con un *lector* es muy sencillo, existen incluso teléfonos móviles que pueden desempeñar esta funcionalidad, por lo que un atacante podría escuchar información sensible de una manera muy sencilla. Se multiplican también el número de posibles atacantes, aparecen nuevos perfiles de adversario. No necesariamente se trata de una persona que trata de atentar a la salud del paciente. Los datos médicos que alberga el *IMD*, o incluso el mero hecho de detectar su presencia, podrían interesar desde a una compañía aseguradora hasta en una entrevista de trabajo.

En [8] se presentan las consecuencias que estos ataques pueden tener sobre el paciente. Si bien no existen incidentes conocidos, dotar de seguridad al *IMD* es importante en tanto en cuanto existen ya en la actualidad ataques probados en laboratorio. Ataques que han conseguido deshabilitar terapias programadas en un *DAI* vía wireless, e incluso inducir un estado de shock en el paciente que lleva implantado un *DAI* [10], o ataques que agoten la batería del *IMD* y le dejen inhabitado.

Para prevenir que esto suceda fuera de un laboratorio ha de pensarse ya en los mecanismos de seguridad que protegerán la siguiente generación de implantes. Estos mecanismos deben ser un compendio de medidas tecnológicas y legales [8]. Tecnológicamente deben adoptarse medidas que eviten accesos y usos no autorizados al *IMD*. En el apartado 4 de este artículo se presenta un resumen de las principales medidas propuestas en este aspecto. Legalmente, entidades reguladoras como la FDA o su equivalente europea *EMA*, deberían promulgar métricas para la evaluación de la seguridad en los *IMDs*.

Emplear soluciones de seguridad clásicas, diseñadas para sistemas computacionales estándares no sirve para cubrir la seguridad en *IMDs* porque: El mero empleo de estas técnicas, como pueden ser las clave pública o privada, no cubren casos de emergencia en los que sea necesaria la comunicación con el *IMD* sin tener la clave de acceso [11]. Por otro lado, los *IMDs* tienen restricciones de almacenamiento (algunos *IMDs* utilizados actualmente disponen solamente de 8KB [10]) y de energía que las técnicas clásicas no contemplan. La batería de un *IMD* es una restricción muy importante a tener en cuenta ya que la batería del dispositivo está pensada para durar años. Reemplazar la batería de estos dispositivos requiere cirugía y puede resultar complicado en algunos casos. De modo que es necesario diseñar nuevos esquemas de seguridad y privacidad que sean eficientes con los recursos de almacenamiento y energía.

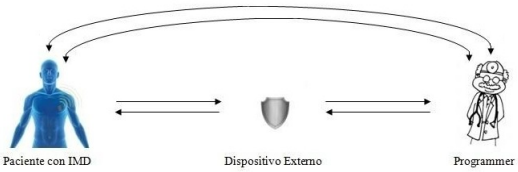

Figura 1. Comunicaciones Dispositivo Externo Implantable

I-D. Estructura del artículo

El artículo está organizado como sigue: En la siguiente sección se presenta el funcionamiento típico de un *IMD* y el principal problema de seguridad que presenta. En la sección 3 se presentan las metas de seguridad y las tensiones existentes que se crean entre éstas. En la sección 4 se presentan las principales soluciones existentes ante los problemas de seguridad encontrados. El artículo concluye en la sección 5.

II. Por qué es Necesaria la Seguridad en Implantes

El *IMD,* como puede verse en la Figura 1, puede comunicarse directamente con el *programador* o puede delegar está función sobre un dispositivo intermedio que autentique al *programador*. En ambos casos, una vez autenticado, el *IMD* responderá a las peticiones del *programador*. Y en un caso de emergencia debe poder responder e incluso ser deshabilitado por el personal médico. Este es el caso de los *DAIs*, que deben ser desactivado antes de una cirugía para evitar un estado de shock en el paciente. Es decir, no siempre deberá comunicarse con un dispositivo ya conocido.

Bajo este escenario de uso, es necesario pensar en la posibilidad de que las señales que reciba el *IMD* no provengan del *programador* y sean malintencionadas, incluso es posible que sea el propio paciente quien sabotee su dispositivo para obtener de él un uso no supervisado. En estos casos, debido a la importante función fisiológica que realizan los implantes, se puede estar poniendo en peligro la integridad física del paciente.

El objetivo principal es encontrar una solución de compromiso que balancee la seguridad entre los dos escenarios posibles:

A. Seguridad en un escenario de uso normal, donde el paciente puede controlar quién interactua con su *IMD*. En este caso se requiere un fuerte control de acceso y el uso de protocolos criptográficos en las comunicaciones con el *IMD* para prevenir el acceso malintencionado o no autorizado al mismo. El *IMD* no debe responder a peticiones de lecturas de datos o de reprogramación del dispositivo. Incluso es deseable que el implante sea indetectable a partes no autorizadas. Una solución que plantee un control de acceso seguro y eficiente debe evitar que un atacante pueda obtener la información del *IMD* y atentar contra la salud del paciente.

B. Seguridad en caso de emergencia. Igual de importante que mantener un fuerte control de acceso e incluso ser

Cuadro I
EFECTOS ADVERSOS EN DIFERENTES TIPOS DE IMD [1]

IMD	Efectos Adversos
Marcapasos y DAIs	Insuficiencia Cardíaca, taquicárdica, arritmia
Sistema de control de extremidades protésicas	Lesiones, daños a la prótesis, movimientos no controlados
Estimulador de la espina dorsal	Perdida en el sistema de alivio del dolor, estimulación inadecuada
Prótesis de retina, lentes intraoculares	Ceguera, distracción, confusión
Bomba de administración de medicación	Administración de dosis inadecuadas
Neuroprótesis	Diversos efectos a nivel neuronal, pérdida de la conciencia
Neuroestimuladores	Estimulación inadecuada
Monitores Implantables o sensores	Lecturas de datos incorrectas
Tatuaje LED	Muestra inapropiada de los datos
Estimulador del nervio Sacral	Infecciones, estimulación inapropiada.

invisible, es el hecho de que sea a la vez fácilmente accesible en casos de emergencia. En un esquema seguro, bajo una situación de emergencia, un médico debe ser capaz de conectarse con el *IMD* del paciente. Supóngase un paciente que entra por la puerta de urgencias. En este caso el personal médico debe ser capaz de comunicarse con el *IMD*, determinar de qué tipo de dispositivo se trata, extraer información fisiológica, de tratamiento, e incluso alterar los parámetros o actualizarlo.

Distinguir entre ambos escenarios no es una tarea trivial para el *IMD*, de ahí la importancia de encontrar soluciones que balanceen la seguridad para proveer seguridad en el primer caso y seguridad física de paciente o protección en el segundo. Sin embargo y ante la duda de que el dispositivo quede inaccesible, es conveniente relajar las condiciones de seguridad, de nada sirve proteger a un paciente de posibles ataques, si puede morir por ello.

El objetivo es encontrar una solución en la que el *IMD* sólo pueda ser accedido por partes autorizadas cuando sea necesario y que permanezca inaccesible e invisible en caso contrario. El cumplimiento de estos dos objetivos crea tensiones entre los objetivos de seguridad. Y de estas tensiones nacen la mayoría de las medidas de seguridad propuestas.

III. VULNERABILIDADES Y TENSIONES

III-A. Vulnerabilidades

Para identificar qué medidas de seguridad se necesitan, es necesario primeramente pensar qué vulnerabilidades tienen los sistemas empleados con *IMDs*.

Con frecuencia se mide la vulnerabilidad/confianza en un sistema conforme al grado de acceso que puede llegar a alcanzar un usuario no autorizado. Es necesario por tanto tener claro cuáles son los roles en el sistema y a quién se considera un usuario no autorizado, teniendo en cuenta que en el caso de un *IMD* la lista de usuarios autorizados es variable [6].

Un ataque puede venir por tres vías [1]:

1. **Proximidad:** El atacante podría explotar el rango de alcance de las comunicaciones tanto para obtener un acceso no autorizado como para realizar escuchas fraudulentas. La proximidad se refiere a la distancia entre el atacante y el *IMD*. La mayoría de las soluciones, como las que basan el control de acceso en esta distancia, plantean acceso al dispositivo sólo a cortas distancias, ya que si la distancia límite es amplia el *IMD* podría verse comprometido en mayor medida.
   Se considera distancia de contacto si es necesario tener contacto físico con el paciente para tener acceso al *IMD*, distancia corta hasta 1 metro y distancia media de 1 a 50 metros.
2. **Actividad:** El atacante podría tratar de alterar el correcto funcionamiento del dispositivo. Los *IMDs* pueden desempeñar diferentes actividades: medir parámetros biomédicos de allí donde estén implantados (medición), tratar una dolencia (actuación), procesar la información a partir de la información recopilada, etc.

   En la Tabla 1 se resumen los ataques que pueden sufrir los diferentes tipos de IMD [1], donde el termino efectos adversos hace referencia a los efectos negativos que aparecen debido a un ataque o explotación de una determinada vulnerabilidad.
3. **Estado:** El atacante podría atacar al *IMD* alterando el estado del paciente. En ciertos *IMDs* el estado actual de un conjunto de parámetros del paciente condicionan que su acceso sea autorizado o no, o incluso puede programarse el *IMD* para que a partir de la señal de un sensor, que mide la tensión de un musculo que el paciente ejercita voluntariamente, empiece una sesión de comunicación o actualización, etc.

III-B. Tensiones

Las tensiones, que nacen de intentar cumplir los diferentes objetivos de seguridad, pueden clasificarse en los siguientes grupos:

- **Seguridad del Dispositivo/Seguridad Física del Paciente:** Bajo condiciones de uso normales, el *IMD* es vulnerable a diversos ataques, incluso a larga distancia debido al uso de comunicación wireless que emplea para recibir peticiones de datos y actualizarse. De manera que debe procurarse un sistema que garantice confidencialidad, integridad y disponibilidad.
  Sin embargo en una situación de emergencia el personal médico debe poder acceder al implante sin restricciones

y de manera rápida.

- **Vida de la Batería/Recursos del IMD:** Los *IMDs* tienen recursos limitados de energía, almacenamiento y cómputo. Éstos funcionan gracias a una batería integrada y para sustituirla es necesario recurrir a la cirugía, lo cual en algunos casos conlleva riesgos asociados. Y recargar la batería mediante campos electromagnéticos externos puede afectar a otros órganos, por lo que no es recomendable, de manera que debe intentarse que la batería dure el máximo número de años posible.
  Luego , en la fase de diseño de la seguridad de estos dispositivos no ha de olvidarse este aspecto y considerar siempre el impacto en la vida de la batería.
- **Tiempo de Respuesta:** Por el mismo motivo, tampoco ha de olvidarse que el *IMD* en una espera larga puede suponer un riesgo para la salud o vida del paciente, por lo que debe medirse la latencia de respuesta de los mecanismos de seguridad implementados y asegurarse que ésta se encuentra dentro de un rango razonable.

IV. CONTRAMEDIDAS

Diferentes (contra)medidas pueden ser llevadas a cabo por el *IMD* para salvar las vulnerabilidades y que conformen una solución de compromiso que mantenga el equilibrio entre las tensiones existentes. Estas medidas pueden considerarse como preventivas, detectivas o correctivas. En esta sección se presentan los principales tipos de medidas propuestas hasta la fecha (véase la Figura 2).

IV-A. Medidas de Notificación

Los sistemas de notificación permiten informar directamente al paciente, mediante una señal de alerta (por ejemplo sonido o vibración), cuando se producen determinados eventos, como por ejemplo cuando el IMD establece una comunicación wireless [6], o cuando alguno de los parámetros biomédicos esta fuera de un rango aceptable, etc. [10].

IV-B. Auditoría

Auditar es una medida detectiva, que registra los accesos autorizados y no autorizados al dispositivo y almacena en detalle el estado del paciente. Supone una medida para detectar acciones no permitidas, y una fuente de evidencia de estas acciones para tomar posteriores acciones correctivas, además actúa como elemento disuasorio.

IV-C. Medidas Criptográficas y Control de Acceso

Las soluciones basadas en métodos criptográficos son adecuadas para proteger los canales de comunicación y los registros almacenados dentro de los dispositivos. Así mismo son utilizadas también para verificar/gestionar el acceso al *IMD* mediante firmas digitales o funciones resumen. Existen protocolos tanto de clave simétrica como de clave pública, siendo estos últimos muchos más costosos computacionalmente hablando.

Algunas soluciones propuestas se basan en el uso de clave simétrica entre los dispositivos del *IBN*. Al emplear esta medida surge el problema clásico de cómo distribuir las claves. La clave de *IMD* podría ser llevada por el paciente en una brazalete externo, sin embargo tenemos el mismo problema que con las aproximaciones basadas dispositivos externos (véase Sección IV-C-B), no quedando contemplado el caso de perdida del brazalete. En este caso, la perdida del brazalete dejaría incomunicado al IMD, pues no se conocería su clave de acceso[12]. Otra solución para portar la clave es la impresión de la misma en el paciente mediante micro-pigmentación ultravioleta (tatuajes invisibles) que pudiera ser leídos por el personal médico en caso de emergencia [13].

Una manera de prevenir el uso no autorizado e inadecuado son las medidas de control de acceso al *IMD*. Las medidas que vienen a continuación se basan en el control de acceso al dispositivo, y su uso no es incompatible con el uso de las anteriores:

A. Soluciones basadas en certificados y listas: Las soluciones basadas en certificados basan la autenticación en la obtención de credenciales en cada sesión de comunicación con el *IMD*. Para que esta solución no comprometiese la seguridad del paciente, sería necesario contar con unas BBDD/estrucuturas PKI accesibles a nivel global a través de Internet. Si un paciente necesita acceso de emergencia a su *IMD* en un país que no es el suyo y el personal médico no consigue los credenciales necesarios, bien por no contar con acceso on-line o por no encontrarse autenticado en la base de datos, no se podrá modificar ni tan siquiera deshabilitar el dispositivo, poniendo muy seriamente en peligro la vida del paciente. Otra desventaja, es que mantener a nivel global las BBDD actualizadas es muy costoso.

En [14] se describen diferentes técnicas de control de acceso dirigidas a evitar los ataques por repetición. Además se plantea como método de evitar la detección del *IMD* la no respuesta a los mensajes de entidades no autenticadas previamente. Para ser indetectable, un *IMD* debería responder solo a lectores autorizados, para ello el lector ha de haberse autenticado previamente.

B. Soluciones de confianza en dispositivos externos: Otras soluciones de control de acceso pasan por el uso de dispositivos externos, esto es, no implantados en el cuerpo del paciente, en los que se delega parte o la totalidad de la seguridad del dispositivo, liberando así también de computo al *IMD*. Esta medida puede clasificarse dentro del grupo de medidas protectivas. Dos ejemplos claros de aplicación son los *Communication Cloaker* y el *RFID Guardian*.

Las ventaja de estas soluciones es que suelen integrarse en un mismo dispositivo (Cloaker/Guardian) diferentes propiedades de seguridad: auditoria, administración de claves, el control de acceso y la autenticación.

C. Soluciones de confianza en dispositivos internos: Esta medida también puede considerarse como preventiva. Consiste en un implantable (*IMD Hub*) que funcione de centro

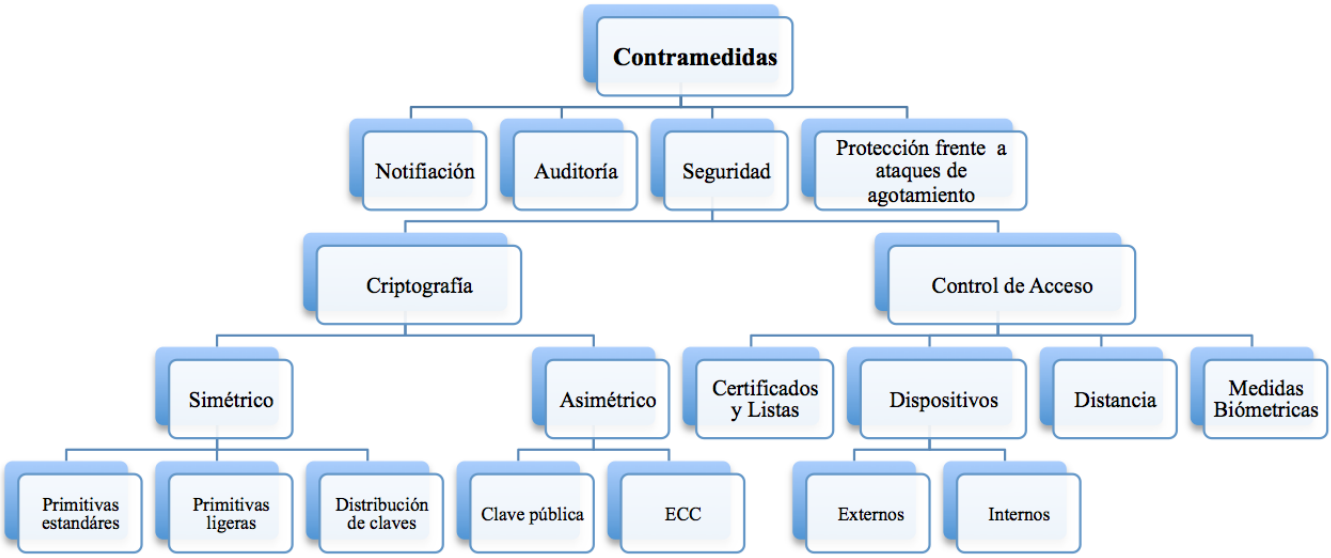

Figura 2. Clasificación Soluciones de Seguridad

de autenticación e interruptor de red para toda la red de dispositivos dentro del *IBN*. Esta aproximación/contramedida tiene la desventaja de confiar en un solo hub central que provea la comunicación, quizás debiera estudiarse la posibilidad de tener dos hub conectados entre sí [15].

D. Soluciones basadas en distancia: Estas soluciones basan el control de acceso en la distancia. Proponen deshabilitar las comunicaciones wireless de larga distancia, permitiendo comunicación solo con dispositivos que puedan demostrar estar en un radio corto [16]. Esto se lleva a cabo en muchos casos haciendo que el *IMD* no este disponible menos que sea activado mediante un interruptor magnético o técnicas similares como puede verse en [17] . Sin embargo, no puede asegurarse que estas soluciones sean seguras, ya que existen estudios que demuestran que campos magnéticos cercanos al dispositivo pueden alterarlo [18].

Un subconjunto de las medidas basadas en distancia, son las llamadas basadas en 'distancia limite'. En [19] se describe un protocolo en el que, además de las operaciones asociadas al cifrado de las comunicaciones, se toman en cuenta los tiempos de respuesta en la sesión actual con el dispositivo, a través de los cuales se calcula la distancia a la que se encuentra el lector. Si la distancia está comprendida dentro del rango definido como próximo, el protocolo continua, de lo contrario se considera que el dispositivo no es próximo al *IMD* y se corta la comunicación con el mismo.

Incorporar una medición de tiempo en los protocolos puede ayudar a evitar los ataques por repetición, ya que el dispositivo podría identificar solicitudes anacrónicas y rechazarlas [14].

Las soluciones basadas en distancia tienen dos deficiencias importantes: 1) Estos esquemas, al basarse en la distancia, comprometen al IMD si el adversario esta dentro del radio delimitado. Sería deseable asegurar la seguridad del paciente independientemente de la distancia a la que se encuentre el atacante, ya que existen posibles situaciones en las que pudiera encontrarse cerca, por ejemplo en transporte público, en el trabajo, o como ya se ha comentado al principio de este articulo, el adversario podría ser el propio paciente, que estaría lo suficientemente cerca de si mismo; y 2) Existen tecnologías que permiten a un adversario extender el rango permitido y comunicarse con el *IMD* aun estando a larga distancia [12].

E. Medidas Biométricas: Se llama Biometría al conjunto de técnicas que se basan en características físicas, tales como huellas dactilares, iris, voz, etc. Éstos son métodos eficaces para proveer autenticación, que permita luego control de acceso u otras funciones de seguridad.

Las técnicas basadas en biometría son mejores, en algunos casos, que las basadas en claves, porque se evita la necesidad de almacenar contraseñas, pero por otro lado suele requerir la presencia física de la persona. Esta desventaja no es tal cosa en el escenario de seguridad en *IMD*, ya que en caso de emergencia, el paciente se encuentra físicamente en la sala de urgencias, pero si sería una desventaja cuando el personal médico intentara acceder de manera remota al *IMD*.

En [20] se propone una solución para permitir acceso seguro, impidiendo un acceso no autorizado, en casos de emergencia. El esquema propuesto se basa en información

biométrica del propio paciente. El acceso al *IMD* se dividiría en dos pasos o niveles. En el nivel 1 se utilizan parámetros biométricos como la huella dactilar, el peso, el color de ojos, etc. Si se supera este primer nivel, se continua con el segundo nivel de autenticación, en el que, para finalmente obtener acceso al dispositivo, es necesario proveer como entrada la información biométrica del iris del paciente. Esta información estará previamente almacenada como una llave en el *IMD*. La autenticación basada en el iris es una de las más precisas y también más rápidas. Además, para registrar correctamente el iris es necesaria una cámara NIR (cámara de proximidad en el infrarojo) a una distancia de entre 50-70 cm frente al paciente, lo cual hace que un ataque a este método sea evidente de reconocer por parte del propio paciente.

IV-D. Medidas contra los Ataques por Agotamiento de Recursos

Basándose en el hecho de que la comunicación wireless de un dispositivo con un lector sigue una serie de patrones observables como la frecuencia en la comunicación, localización, etc., en [21] se presenta un esquema de seguridad contra los ataques por agotamiento de recursos utilizando Support Vector Machines (SVMs) que corren en el teléfono móvil del paciente. Los autores han considerado cinco datos mediante los cuales el algoritmo de clasificación empleado determina si la comunicación entrante sigue un patrón de acceso al IMD, o no. De esta manera se detectan posibles ataques. Así por ejemplo, si cierto tipo de acciones siempre son realizadas desde la consulta del médico, se considerará un intento de ataque que un lector intente realizar dicha acción desde otra localización.

Los principales problemas de esta solución son que: 1) Esta solución se basa en el funcionamiento normal del *IMD*, no contemplando situaciones de emergencia, en la que pueden incumplirse todos los patrones de acceso. En este caso el algoritmo negaría el acceso de manera irrevocable con las posibles consecuencias que esto conlleva; 2) Necesita de un elemento externo como es el teléfono móvil, lo cual implica las desventajas vistas en la sección IV-C-B; y 3) Se asume la capacitación del paciente para decidir sobre si una petición de acceso es o no válido.

V. Conclusiones

En este artículo se han presentado los principales problemas de seguridad que presentan los dispositivos médicos implantables a día de hoy. Y se ha visto que esto puede conllevar importantes riesgos en la salud de los pacientes que los utilicen. Queda en evidencia - y sin querer ser alarmistas - la necesidad de dotar de mecanismos de seguridad a estos dispositivos (*IMDs*). Para ello el campo de la Bioingeniería y la Computación deben trabajar conjuntamente para garantizar tanto la seguridad física del paciente como la seguridad de la información.

Referencias

[1] J. Hansen and N. Hansen. A Taxonomy of Vulnerabilities in Implantable Medical Devices. En *P*roceedings of the second annual workshop on Security and privacy in medical and home-care systems (SPIMACS '10), pp. 13-20. ACM, 2010.

[2] Medtronics Inc. http://www.medtronic.com/your-health/bradycardia/device. Consultado Marzo 2012.

[3] T. Denning, Y. Matsuoka and T. Kohno. Neurosecurity:Security and privacy for neural devices. En *N*eurosurgical Focus, vol. 27(1), pp. E7, 2009.

[4] J. G. Webster. Design of cardiac pacemakers. IEEE Press, 1995.

[5] D. Panescu. Emerging technologies: wireless communication systems for implantable medical devices. En *E*ngineering in Medicine and Biology Magazine, vol. 27(2), pp. 96-101, 2008.

[6] D. Halperin, T. S. Heydt-Benjamin, K. Fu, T. Kohno and WH. Maisel. Security and Privacy for Implanted Medical Devices. En *I*EEE Pervasive Computing, vol. 7, pp. 30-39, 2008.

[7] W. Maisel. Safety issues involving medical devices. En *J*ournal of the American Medical Association, vol. 294, pp. 955-958, 2005.

[8] K. Fu. Inside Risk: Reducing risks of implantable medical devices. En *C*ommunications of the ACM, vol. 52, pp. 25-27, 2009.

[9] FDA. http://www.fda.gov/MedicalDevices/Safety/default.htm. Consultado Abril 2012.

[10] D. Halperin, T. S. Heydt-Benjamin, B. Randsford, S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno and WH. Maisel. Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses. En *I*EEE Symposium on Security and Privacy, pp. 129-142, 2008.

[11] S. Gupta, T. Mukherjee and K. Venkatasubramanian. Criticality Aware Access Control Model for Pervasive Applications. En *P*roc. of the Fourth Annual IEEE Pervasive Computing and Communications, pp. 251–257. IEEE Computer Society, 2006.

[12] K. Fotopoulou and B. Flynn. Optimum antenna coil structure for inductive powering of passive RFID tags. En *I*n IEEE International Conference on RFID, pages 71-77, 2007.

[13] S. Schechter En *M*icrosoft Technical Report – MSR-TR-2010-33, 2010.

[14] E.Freudenthal, R.Spring and L.Estevez. Practical techniques for limiting disclosure of RF-equipped medical devices. En *E*ngineering in Medicine and Biology Workshop, pp. 82-85, 2007.

[15] T. Denning, K. Fu and T. Kohno. Absence makes the heart grow fonder: New directions for Implantable Medical Device Security. En Proceedings of the 3rd conference on Hot topics in security (HOTSEC'08), pp. 5:1–5:7. USENIX, 2008.

[16] M. Rieback, B. Crispo and A. Tanenbaum. RFID Guardian: A battery-powered mobile device for RFID privacy management. En *P*roc. 10-th Australasian Conf. On Information Security and Privacy (ACISP'05), vol. 3574 of LNCS, pp. 184-194. Springer-Verlag, 2005.

[17] S. Chekmenev, K. Venkatasubramanian and S.Gupta BioSec: A Biometric based approach for security communication in wireless networks of biosensors implanted in the human body. En *I*CPP Workshops. IEEE Computer Society, 2003.

[18] S. Lee, K. Fu, T. Kohno, B. Ransford, and WH. Maisel. Clinically significant magnetic interference of implanted cardiac devices by portable headphones. En *H*earth Rhythm, vol 6(10), 2009.

[19] K. Rasmussen, C. Castellucia, T. Heydt-Benjamin and S. Capkun. Proximity-based Access Control for Implantable Medical Devices. En *P*roceedings of the 16th ACM conference on Computer and communications security (CCS'09), pp. 410-419. ACM, 2009.

[20] X. Hei and X.Du. Biometric-based two-level secure access control for implantable medical devices during emergencies. En *I*EEE Infocom, pp. 346-350, 2011.

[21] X. Hei, X. Du, J. Wu and F. Hu. Defending resource depletion attacks on implantable medical devices. En *P*roc. Of the Globlecom, pp. 1-5, 2010.