XXII Seminario de Ingeniería Biomédica
Núcleo de Ingeniería Biomédica
Facultades de Medicina e Ingeniería
UdelaR

Seguridad en dispositivos médicos implantables (IMDs)

Leonardo Etcheverry

letcheve@fing.edu.uy

Resumen— Este trabajo presenta un breve relevamiento de problemas de seguridad detectados en dispositivos médicos implantables (como bombas de insulina y cardiodefibriladores) con comunicación inalámbrica . Un agente malicioso puede explotar estos problemas de seguridad para obtener información confidencial del paciente que lleva el implante o, en algunos casos, poner en peligro su vida. En primer instancia se resumen los resultados de dos publicaciones en las que se demostraron ataques exitosos. La primera es el caso de una bomba de insulina, la segunda un cardiodefibrilador implantable (ICD). Como aporte original se analizan además los potenciales problemas de seguridad de un sistema de páncreas artificial utilizado en un estudio recientemente publicado.

1. Introducción

Las continuas mejoras tecnológicas en biosensores, procesadores embebidos de bajo consumo y comunicaciones inalámbricas en los últimos años han permitido la producción de nuevos dispositivos médicos implantables (IMDs, *Implantable Medical Devices*) de mayor complejidad y prestaciones.
Dispositivos implantables como marcapasos, cardiodefibriladores (ICDs), implantes cocleares y bombas de insulina son ahora capaces de comunicarse con el mundo exterior.
Esta capacidad de comunicación permite a médicos monitorear remotamente el funcionamiento de implantes e indicadores de salud del paciente, resultando en un mejor seguimiento de las terapias y mejorando la calidad de vida de los pacientes. Además de las funciones de telemetría, muchos de estos dispositivos pueden ser ahora programados y controlados en forma inalámbrica, ofreciendo gran comodidad a la hora de establecer diferentes parámetros de funcionamiento para cada terapia.
En oposición a estas ventajas aparece el problema de la seguridad de estos implantes conectados. Un agente malintencionado (adversario) puede ahora comprometer la confidencialidad, integridad y disponibilidad de un dispositivo, con consecuencias que van desde la violación de la privacidad del paciente hasta su exposición a una situación que ponga en peligro su vida.

Este trabajo expone ejemplos de problemas de seguridad de IMDs ya documentados en la literatura científica, con el objetivo de comunicar la necesidad de investigar aspectos de seguridad en el diseño y uso de implantables. Además, como aporte original, se realiza un breve análisis de potenciales vulnerabilidades de un sistema de páncreas artificial utilizado en un estudio recientemente publicado[1].

Si bien los inminentes problemas de seguridad de dispositivos embebidos conectados han sido estudiados en el pasado[2], los dispositivos médicos implantables presentan desafíos de seguridad característicos que aún se presentan como problemas abiertos. Un claro ejemplo es el uso de criptografía para proteger las comunicaciones entre IMDs. Si bien ciertas soluciones criptográficas son conocidas y utilizadas en dispositivos embebidos, su utilización puede requerir una potencia de cómputo y consumo de energía que vuelve inviable su uso en un implantable.
El uso en un marcapaso de funciones criptográficas que impongan un consumo energético no despreciable resultaría en una vida de batería más corta. Una vida de batería más corta se traduciría en la necesidad de realizar la riesgosa y costosa intervención de implantar un nuevo marcapasos con mayor frecuencia. Otro ejemplo de un problema característico es la necesidad de que ciertos sistemas sean *fail open*. Un sistema *fail open* debe errar en permitir el acceso a un dispositivo. Por ejemplo, una persona con un cardiodefibrilador implantado (ICD) sufre un accidente y debe ser intervenido

quirúrgicamente en un caso de emergencia. El equipo médico debe ser capaz de desactivar el ICD para poder trabajar con seguridad. Si el proceso de autorización para comunicarse con el ICD presenta una falla, el sistema debería entrar en un estado *fail open* en el cual se le permita al equipo médico desactivar el dispositivo.
Esta tensión entre utilidad y seguridad en el diseño de IMDs ha sido presentada en otros trabajos[2]–[4] y no se discutirá aquí.

2. Desarrollo

2.1. Ataque a una bomba de insulina

Esta sección describe un ataque sobre un sistema formado por un monitor continuo de glucosa en sangre (GCM) y una bomba de infusión de insulina publicado en 2008[5] por Li et al.

Una bomba de insulina es un dispositivo usado para administrar una dosis de insulina a pacientes diabéticos que la necesiten. La bomba es un dispositivo que almacena la insulina y, bajo el control de un sistema electrónico, administra la inyección de insulina a través de un catéter y una cánula implantada en forma subcutánea. La bomba puede ser programada para entregar la insulina en forma automática de forma de controlar la glucosa en sangre entre comidas y mientras la persona duerme. Además, el usuario puede controlar la bomba directamente e indicarle que administre una dosis cuando come. La bomba tiene una interfaz de usuario capaz de desplegar información útil al paciente, como por ejemplo una historia su funcionamiento.

Además, las bombas muchas veces incluyen un control remoto inalámbrico para mayor comodidad del usuario. Dado que el usuario de la bomba necesita monitorear su nivel de glucosa en sangre, algunos sistemas de infusión de insulina incluyen la capacidad de integrar un monitor continuo de glucosa o GCM. Un GCM está compuesto por un sensor subcutáneo que mide el nivel de glucosa en sangre y lo transmite a un receptor en forma inalámbrica. Este receptor puede ser otro dispositivo capaz de desplegar el valor medido al usuario o puede ser la misma bomba de insulina.
La comunicación inalámbrica entre los elementos de este sistema presenta a un potencial adversario la oportunidad de interferir con el funcionamiento normal del la bomba.

Li et al. demuestran como vulnerabilidades en la implementación del enlace de comunicación inalámbrico entre el control remoto y una bomba disponible comercialmente permiten atacar con éxito la confidencialidad, integridad y disponibilidad del sistema. Un primer ataque pasivo consiste en la intercepción de la comunicación enviada desde el control remoto hacia la bomba utilizando un equipo de recepción Universal Software Radio Peripheral[6] (USRP) de bajo costo normalmente utilizado en aplicaciones de Software Defined Radio (SDR). Habiendo interceptado la comunicación, los investigadores encontraron que los datos se enviaban sin encriptarse. Esto permite a cualquier atacante pasivo detectar la presencia del equipo a una distancia de hasta 10m; afectando así la privacidad del paciente.

Su trabajo continuó con la realización de ingeniería inversa del protocolo de comunicación con el objetivo de realizar ataques activos sobre el sistema. En un ataque activo el adversario busca inyectar nuevos mensajes o modificar mensajes legítimos en la comunicación con el objetivo de afectar la integridad del sistema. Un primer ataque demostrado fue lo que en seguridad se conoce como un ataque de *replay*: interceptar un mensaje legítimo e inyectarlo nuevamente en el futuro. Si el receptor acepta este mensaje como válido; el sistema es vulnerable a ataques de *replay*.
Por ejemplo, un adversario puede esperar a que el paciente use su control remoto para administrar una dosis de insulina al momento de comer y capturar ese mensaje. Un tiempo después, el adversario puede volver a enviar ese mensaje (*replay*) y hacer que la bomba inyecte otra dosis de insulina. El ataque también puede ser más sutil, por ejemplo interceptando un mensaje entre el GCM y la bomba de insulina que indique un valor de glicemia alto para luego hacer *replay* de este mensaje en el futuro y así informar al paciente un valor incorrecto de glicemia.

Finalmente se demuestra un ataque en el cual el equipo USRP se hace pasar por el control remoto para transmitir comandos arbitrarios a la bomba de insulina. Así, un adversario podría: (1) detener la

inyección de insulina y provocar un aumento de glicemia, (2) inyectar una dosis de insulina con la posibilidad de provocar un episodio hipoglicémico en el paciente y poniendo en peligro su vida.

El trabajo también propone un par de soluciones de con el objetivo de mitigar estos problemas de seguridad. Una de las posibles soluciones es utilizar un sistema criptográfico simétrico basado en *rolling codes* para proteger la comunicación entre bomba, control remoto y GCM. Otra solución propuesta es la eliminación de la comunicación inalámbrica en favor de utilizar el mismo cuerpo humano como medio de transmisión (*Body Coupled Communication*).
Más allá de las soluciones propuestas, el trabajo de Li et al. deja en evidencia como un IMD disponible en el mercado es vulnerable a ataques de baja sofisticación.

2.2. Ataque a un cardiodefibrilador implantable (ICD)

Un cardiodefibrilador implantable o ICD es un dispositivo que permite corregir alteraciones del ritmo cardíaco mediante la aplicación de estímulos eléctricos. A diferencia de un marcapasos, un ICD puede administrar pulsos eléctricos de mayor energía para corregir arritmias peligrosas. Normalmente son implantados bajo la piel en el pecho, con electrodos conectados al corazón. Un ICD monitorea el ritmo cardíaco en forma continua y puede decidir aplicar un pulso eléctrico para corregirlo.
Una vez implantado, un profesional de la salud puede utilizar un equipo programador externo, que se comunica con el ICD con la finalidad de escribir o leer información de identificación, establecer parámetros de funcionamiento para cada terapia, realizar diagnósticos y auditar la historia de funcionamiento del dispositivo y signos vitales del paciente. La comunicación entre programador e ICD se realiza en forma inalámbrica por radiofrecuencia.

En una publicación de 2008[7] Halperin et al. muestran ejemplos de ataques a la seguridad de un ICD comercializado en 2003.
Su trabajo muestra como la intercepción de la comunicación entre un programador y un ICD puede ser utilizada en ataques de *replay* para comprometer la confidencialidad, integridad y disponibilidad del ICD. Como ejemplo, los investigadores muestran como el *replay* de un mensaje de consulta por parte del programador hacia el ICD logra provocar la respuesta del ICD con datos del paciente como nombre, enfermedad, y otros datos sensibles comprometiendo así la privacidad de la persona. Más interesante aún es el ataque en que se hace replay de comandos para deshabilitar terapias. Un ICD con terapias deshabilitadas dejará de actuar aún cuando el corazón presente una situación que amerite la aplicación de un estímulo eléctrico.
Por último, los investigadores reportan la posibilidad de hacer un *replay* de un comando que pone al ICD en un modo de test capaz de inducir una fibrilación en el corazón. Este modo de test es normalmente utilizado en la intervención de implantación del ICD para verificar que el dispositivo es capaz de detectar la fibrliación y actuar en consecuencia proporcionando un shock de defibrilación.

Si bien en este trabajo los investigadores se limitaron a comunicarse con un ICD desde distancias de pocos centímetros, la presencia de estas vulnerabilidades sigue siendo relevante ya que existe creciente interés en extender el alance de la comunicación de ICDs, por ejemplo usando la banda MICS[8]. Extender el alcance traería ventajas como facilitar el monitoreo del funcionamiento del dispositivo: una persona puede tener una base receptora de telemetría en su hogar encargada de retransmitir información del paciente a una clínica. Varios productos con esta funcionalidad ya se encuentran disponibles en el mercado[9], [10].

2.3. Potenciales vulnerabilidades en un páncreas artificial.

Un estudio médico[1] recientemente publicado analiza el diseño y uso de un páncreas artificial con el objetivo de mantener el nivel de glicemia en pacientes con diabetes tipo I en forma automática.
El páncreas artificial diseñado está formado por un medidor continuo de glicemia (GCM), una bomba de insulina y un sistema de control realizado en software que cierra el lazo. A diferencia del caso de una bomba de insulina comandada por el paciente, en este caso es el sistema de control quien ajusta las dosis de insulina de acuerdo al valor de glicemia sensado.

En particular, la plataforma elegida para ejecutar el software de control fue un *smartphone* (iPhone4S). La utilización de un dispositivo de propósito general como un iPhone es una buena oportunidad para intentar analizar los problemas de seguridad que podrían aparecer a medida que los dispositivos implantables se vuelven más complejos y conectados. El estudio probó el funcionamiento del sistema en 50 personas durante un tiempo de 5 días.

Por un lado un smartphone presenta varias características que lo hacen atractivo para este tipo de aplicaciones: (1) es un dispositivo personal que siempre acompaña a la persona, (2) ofrece una interfaz de usuario programable que puede ajustarse a cada aplicación particular, (3) el dispositivo ya resuelve funciones de comunicación y (4) es un dispositivo de cómputo de propósito general.
Por otra parte, al igual que cualquier sistema de propósito general conectado a la red, es un dispositivo potencialmente vulnerable a problemas de seguridad.

En esta sección se evalúan algunos de los potenciales problemas de seguridad en esta solución.

Escenarios potenciales que comprometen la seguridad del sistema:

- una aplicación maliciosa no interactúa de ninguna forma con la aplicación de control del páncreas artificial, pero consume batería del teléfono limitando su disponibilidad.
- una aplicación maliciosa utiliza todo el ancho de banda de comunicaciones del dispositivo, impidiendo la transmisión de telemetría por la red.
- una aplicación maliciosa implementa un ataque de "side-channel" sobre la aplicación de control del páncreas artificial. Por ejemplo, usando tiempos de ejecución para ganar información sobre el estado de la aplicación de control.
- una aplicación maliciosa que escape de su entorno seguro de ejecución (*sandbox*) podría potencialmente:
    - comunicarse con el GCM, obtener valores de glicemia de la persona y reportarla a terceros.
    - comunicarse con la bomba de insulina y administrar una dosis para provocar un episodio hipoglicémico (posiblemente bajo control de un adversario remoto)
    - interferir con el funcionamiento normal del proceso responsable de ejecutar el algoritmo de control del páncreas artificial.
    - modificar los registros históricos de la aplicación de páncreas artificial; impidiendo su correcta auditoría.
    - impedir la comunicación del paciente con el mundo exterior cuando se detecte un episodio hipoglicémico.
    - combinar información de posicionamiento (GPS) y control de la bomba de insulina para provocar un episodio hipoglicémico cuando el paciente está en lugar alejado, moviéndose en un vehículo, etc.

En estos escenarios se puede apreciar el potencial efecto sobre la confidencialidad, integridad y disponibilidad del sistema de páncreas artificial implementado. Las consecuencias, como es característico en los sistemas implantables[4], van desde la violación de la privacidad del paciente hasta situaciones que pueden poner en riesgo su vida.

Si bien la implementación del páncreas artificial en un smartphone rara vez se daría fuera de un prototipo, es importante ver que los problemas de seguridad son en buena parte consecuencia de la ejecución de software en un dispositivo de propósito general. A medida que los dispositivos médicos implantables vayan ganando complejidad y necesidad de ejecutar algoritmos de control o telemetría más sofisticados; sus implementaciones migrarán hacia plataformas de propósito general.

3. Conclusiones

Este trabajo muestra la importancia de la investigación en la seguridad de dispositivos médicos, especialmente en IMDs. El impacto directo que un problema de seguridad en un dispositivo médico implantable puede tener sobre la integridad física de la persona implica que la seguridad debe ser un aspecto siempre presente en su diseño, desarrollo y estudio. La seguridad de un IMD debe ser tenida en cuenta desde la concepción de un producto y en todas sus fases de desarrollo.

La detección de potenciales vulnerabilidades y la creación de modelos de amenazas es un trabajo especializado que debe ser llevado adelante por profesionales en el área de seguridad. Al mismo tiempo, la tensión entre utilidad y seguridad en estos dispositivos marca que todos los integrantes de un equipo multidisciplinario (médicos, ingenieros, gerentes de proyecto) deben tener presente esta problemática. Finalmente, aún cuando no se han detectado ataques en el campo como los demostrados en los trabajos mencionados, es importante tener presente su potencial impacto y así intentar prevenir y mitigar estos incidentes.

4. Bibiografía

[1] S. J. Russell, F. H. El-Khatib, M. Sinha, K. L. Magyar, K. McKeon, L. G. Goergen, C. Balliro, M. A. Hillard, D. M. Nathan, and E. R. Damiano, "Outpatient Glycemic Control with a Bionic Pancreas in Type 1 Diabetes," *N. Engl. J. Med.*, vol. 0, no. 0, p. null, 2014.

[2] M. M. Kermani, M. Zhang, A. Raghunathan, and N. K. Jha, "Emerging Frontiers in Embedded Security," in *VLSI Design and 2013 12th International Conference on Embedded Systems (VLSID), 2013 26th International Conference on*, 2013, pp. 203–208.

[3] M. Rostami, W. Burleson, A. Juels, and F. Koushanfar, "Balancing security and utility in Medical Devices?," in *Design Automation Conference (DAC), 2013 50th ACM / EDAC / IEEE*, 2013, pp. 1–6.

[4] D. Halperin, T. S. Heydt-Benjamin, K. Fu, T. Kohno, and W. H. Maisel, "Security and Privacy for Implantable Medical Devices," *IEEE Pervasive Computing*, vol. 7. pp. 30–39, 2008.

[5] C. Li, A. Raghunathan, and N. K. Jha, "Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system," in *2011 IEEE 13th International Conference on e-Health Networking, Applications and Services, HEALTHCOM 2011*, 2011, pp. 150–156.

[6] "Ettus Research - Products." [Online]. Available: https://www.ettus.com/product. [Accessed: 23-Jun-2014].

[7] D. Halperin, S. S. Clark, K. Fu, T. S. Heydt-Benjamin, B. Defend, T. Kohno, B. Ransford, W. Morgan, and W. H. Maisel, "Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses," *Proc. - IEEE Symp. Secur. Priv.*, pp. 129–142, May 2008.

[8] H. S. Savci, A. Sula, Z. Wang, N. S. Dogan, and E. Arvas, "MICS transceivers: regulatory standards and applications [medical implant communications service]," *Proceedings. IEEE SoutheastCon, 2005.*, 2005.

[9] St Jude Medical, "Merlin@home^{TM} Transmitter." [Online]. Available: http://professional.sjm.com/products/crm/connectivity-remote-care/remote-care/merlin-home-transmitter. [Accessed: 23-Jun-2014].

[10] Medtronic, "Medtronic CareLink Network - Living with a Pacemaker." [Online]. Available: http://www.medtronic.com/patients/bradycardia/living-with/carelink/carelink-network/index.htm. [Accessed: 23-Jun-2014].