Universidad de Buenos Aires

Facultades de Ciencias Económicas,

Cs. Exactas y Naturales e Ingeniería

Carrera de Especialización en Seguridad Informática

Trabajo Final de la Especialización

Vulnerabilidades

Análisis de Vulnerabilidades de Ciberseguridad en Desfibriladores Cardíacos Implantados

Autor:

Karina del Rocío Gaona Vásquez

Tutor del Trabajo Final:

Pedro Hecht

2018

Cohorte 2017

2. Declaración jurada de origen de los

Contenidos

“Por medio de la presente, el autor manifiesta conocer y aceptar el Reglamento de Trabajos Finales vigente y se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual”.

_____

Karina del Rocío Gaona Vásquez

DNI: 95703800

Contenido

I. Introducción

La creciente evolución de la tecnología en el internet de las cosas supone también una evolución en la seguridad de los dispositivos, si bien el estar conectados nos proporciona muchos beneficios también conlleva una mayor complejidad en las comunicaciones por lo que la aparición de nuevas vulnerabilidades y ataques también se hacen presentes. [1]

El acceso a personas mal intencionadas es la principal preocupación en el internet de las cosas en donde la seguridad informática de la mayoría del dispositivo se encuentra baja o nula, lo cual podría ocasionar daños muy serios, no solo ya a un nivel de robo de información sino también a un nivel físico.

La medicina incorpora nuevos aparatos para mejorar la salud de las personas y es allí donde damos un foco principal a este trabajo.

Se presentan varios estudios expuestos en un orden cronológico denotando la evolución de los mismos, en donde se expondrán vulnerabilidades, amenazas y ataques que se pueden llegar a realizar.

Se consideran aspectos técnicos como la presentación de vulnerabilidades en un cuadro y aspectos sociales, la preocupante lentitud con que la seguridad va tomando importancia, las normas reguladoras que actualmente existen sobre la telemetría para dispositivos médicos. También se mencionan las similitudes entre los ICD y la falta de una estandarización que asegure un comportamiento común y seguro entre todos los proveedores de estos dispositivos.

Por último, se exponen propuestas para mejorar la seguridad de estos dispositivos con un enfoque situacional que pueda presentar el paciente y el médico en una situación de emergencia.

II. Glosario

Antena: Es aquel dispositivo que permite la recepción y el envío de ondas electromagnéticas hacia un espacio libre. [2]

Asistolia: Ausencia total de sístole cardiaca, con pérdida completa de la actividad. Es una de las formas de paro cardiaco. [3]

Bombas de Insulina: La bomba es un pequeño aparato (más pequeño que muchos móviles) que introduce pequeñas cantidades de insulina en su cuerpo todo el día gracias a un mecanismo para la infusión de insulina. Puede ayudar a gestionar mejor la necesidad de ajustar la dosis de insulina, en especial después de las comidas y durante la noche, y así contribuye a lograr un mejor control de la glucosa. [4]

Codificación NRZI: codifica los datos mediante la presencia o ausencia de transición al principio del intervalo de duración del bit (las transiciones se realizan cuando se desea transmitir un 1 binario). [5]

DAQ: Sistema de Adquisición de datos

DPSK: Modulación de cambio de fase diferencial

EFD: Delimitadores Final de la Trama o su significado en inglés End-of-Frame Delimiters

EKG: Electrocardiograma

EMG: La electromiografía es un estudio que observa la manera en que trabajan juntos los músculos y los nervios. Los nervios llevan mensajes hacia y desde los músculos. Si los nervios o los músculos están dañados, estos últimos podrían funcionar incorrectamente. [6]

FCC: Comisión Federal de Comunicaciones

FDA: Administración de Alimentos y Medicamentos de los Estados Unidos

FSK: Modulación por desplazamiento de frecuencia

IBN: Intra Body Network

ICD: su significado en inglés Implantable Cardioverter Defibrillators ICD and Pacemakers y en español Desfibrilador Cardiaco Implantado

IMD: su significado en inglés Implantable Medical Devices (IMDs) y en español Dispositivo Médico Implantable o sus siglas en español DAI: Dispositivo Médico Implantable

JACC: Revista del Colegio Americano de Cardiología o su significado en ingles Journal of the American College of Cardiology

LSFR: Registro de Desplazamiento con Retroalimentación Lineal

NRZI: No retorno de Zero Invertido o sus siglas en inglés No-Return-to-Zero Inverted.

Osciloscopio: La función principal del osciloscopio es presentar los valores de las señales eléctricas, en forma de coordenadas, a través de una pantalla. [7]

Radio de GNU: Es un conjunto de herramientas de desarrollo de software libre y de código abierto que proporciona bloques de procesamiento de señales para implementar radios de software. [8]

RF: Radio Frecuencia

SFD: Delimitadores de Inicio de Trama o su significado en inglés Start of Frame Delimiters

SOF: Inicio de Trama

Telemetría: La telemetría es la medición o registro de procesos y eventos electrocardiográficos a distancia. [9]

USRP: Universal Serial Radio Periférico

III. Marco Teórico

1. Principios Generales

1.1 Dispositivos Médicos Implantables

Los IMD son dispositivos electrónicos permanentes o semipermanentes implantados dentro del cuerpo humano para tratar una condición médica, que controla el estado o mejora el funcionamiento de alguna parte del cuerpo o simplemente proporciona al paciente capacidades que no poseía antes.

Los modelos actuales de IMD incluyen marcapasos y desfibriladores para monitorear y tratar afecciones cardiacas; neuroestimuladores para la estimulación cerebral profunda. Para casos como epilepsia, parkinson o sistemas de administración de droga están las bombas de infusión; y una variedad de biosensores.

Algunos de los IMD más recientes han comenzado a incorporar numerosas funciones de comunicación y redes usualmente conocidas como “telemetría”, así como capacidades informáticas cada vez más sofisticadas. Esto da como resultado implantes con mayor inteligencia y pacientes con más autonomía. El personal médico puede acceder a los datos y reconfigurar los implantes de forma remota, es decir sin la presencia del paciente además de una significativa reducción de costos.

Las capacidades de telemetría e informática también permiten a los proveedores de atención médica monitorear constantemente el estado de salud del paciente para así poder desarrollar nuevas técnicas basadas en IBN sobre los dispositivos médicos. [10] [11] [12]

1.2 Problemática de Ciberseguridad de los IMDs

La definición de ciberseguridad es “la protección de las redes informáticas que contienen la penetración y de daños o interrupciones”. En el campo médico, la ciberseguridad se refiere específicamente a la integración de dispositivos médicos, redes de computadoras y software. [13]

La mayoría de los beneficios antes mencionados de los IMD ofrecen llevar una vida sana, pero se ha descuidado a la seguridad informática de los dispositivos, se ha ignorado los numerosos riesgos de ciberseguridad que afecta a la privacidad y la salud del paciente. Esto puede llegar a la pérdida de vida de una persona por una vulnerabilidad no considerada en su diseño.

En 2013, el hacker Barnaby Jack declaró que podía tomar control de un marcapasos desde una distancia de poco más de 15 metros y utilizar el aparato para causar un shock letal. El ex vicepresidente de Estados Unidos, Dick Cheney, le ordenó a un médico que eliminara la capacidad inalámbrica de su marcapasos para protegerse de los hackers a pesar de que esto significaba que las actualizaciones de software se debían realizar por medio de una cirugía. [14]

Los IMDs suelen ser viejos y desactualizados y por lo tanto más vulnerables a un ataque. Hasta ahora no ha habido casos de ataques de hackers a pacientes aprovechando las fallas de estos dispositivos. Sin embargo, la FDA y otras agencias se preocupan de lo que podría pasar con estos dispositivos en el futuro. En enero del 2017 la FDA publicó una advertencia donde explicó que ciertos implantes cardiacos podrían ser hackeados y reprogramados para mandar señales y producir un shock que cause la muerte. [14]

La empresa Johnson & Johnson fue obligada a decirle a sus clientes que sus bombas de insulina tenían un fallo de seguridad y que los hackers podían acceder a la bomba de insulina para administrar una sobredosis potencialmente mortal. [14]

Cuanto más dispositivos tengan la capacidad de comunicarse de forma inalámbrica será mayor la preocupación de hackeó, los fabricantes están empezando a poner más atención a estos problemas, están empezando a contratar a expertos en ciberseguridad y creando escenarios de ataque para que los “hackers buenos” reporten los fallos.

1.3 Criterios de Seguridad Informática en IMDs

La confidencialidad, la disponibilidad y la integridad se consideran en un sistema para que sea seguro. En términos de seguridad, los IMD solo deben ser accesibles a las personas autorizadas como médicos autenticados, y cualquier acceso al IMD es responsabilidad de la persona que accedió en caso de una disputa médica. En cuanto a la privacidad, los datos fisiológicos y los datos de tratamiento del paciente deben mantenerse confidenciales en la transmisión inalámbrica. Integridad garantiza que los datos críticos no puedan ser modificados por entidades no autorizadas y que se pueda verificar su origen. [15]

1.4 Historia del ICD

El ICD se ha convertido en los últimos años en una de las principales opciones de tratamiento en los pacientes con arritmias ventriculares malignas, muerte súbita cardiaca o elevado riesgo de desarrollarlas.

Michel Mirowski médico de origen polaco, en 1969 construyó el primer prototipo de ICD junto al DR. Morton Mower en el sótano del Hospital Sinaí en Baltimore en EEUU.

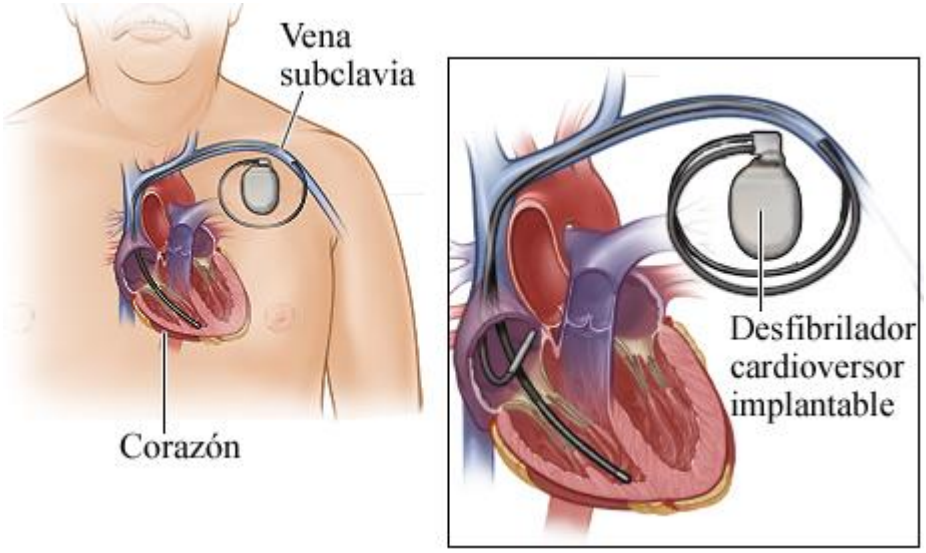
Después de las opiniones tan opuestas de algunos compañeros, la falta de subvenciones y la oposición de las autoridades del momento conoció al Dr.Stephen Heilman en 1972 médico, ingeniero y empresario que lo apoyó y creó una compañía Intec System, dedicada únicamente al desarrollo del desfibrilador cardíaco implantable. Tras cuatro años de experimentar con animales, el 4 de febrero de 1980 junto con los Dres. Reid y Mower implantaron el dispositivo con éxito a una mujer californiana de 57 años que padecía taquicardia ventricular recurrente, en el Johns Hopkins Hospital Center de Baltimore, en EEUU [16], en España el primer ICD se implantó en 1985.

En la primera generación la tecnología de los dispositivos era escasa y no permitía la programación del mismo, el cual solo suministraba choques de alta energía cuando era necesario, con una vida útil de apenas de un año y medio, detectaban únicamente la fibrilación ventricular (FV) (aproximadamente del tamaño de un paquete de cigarrillos) [17], no eran programables de modo que se tenían que encargar a la medida para cada

paciente en particular. [16]. Implantarlos requería una cirugía mayor a corazón abierto, seguida de una larga estadía en el hospital.

La segunda generación aparece en 1988 con un modelo programable, el cual permitía la comunicación inalámbrica, en 1993 se reduce el tamaño de los ICDs. En la actualidad la tercera y cuarta generación, la implantación es fácil, su durabilidad puede alcanzar 6-8 años.

1.5 Desfibriladores cardiacos implantados



Fuente: https://espanol.kaiserpermanente.org/static/health-encyclopedia/es-us/kb/zm63/83/zm6383.shtml

Figura. 1 Desfibrilador cardiaco implantable**.**

Es un dispositivo que monitorea los ritmos cardiacos del corazón y su función principal es detectar alguna anomalía, cuando pasa esto envía un choque eléctrico al corazón que devuelve su funcionamiento a su ritmo normal. Adicionalmente posee marcapasos incorporado que regula el ritmo si los latidos son muy lentos.

Los nuevos modelos están equipados con sensores de presión capaces de monitorear activamente los cambios que podrían llevar a una falla cardíaca. Esto permite alertar al paciente o al personal médico si se detecta un incremento de presión en el ventrículo, ya que representa una condición peligrosa para el paciente.

Los implantes cardíacos también pueden estar equipados con acelerómetros para medir el nivel de actividad física del paciente. Esto se puede configurar como un parámetro de entrada para el controlador del

IMD, lo que permite ajustar la frecuencia de estimulación cardíaca a la que mejor se adapte a cada uno momento. [18]

1.6 Arquitectura y Funcionamiento del ICD

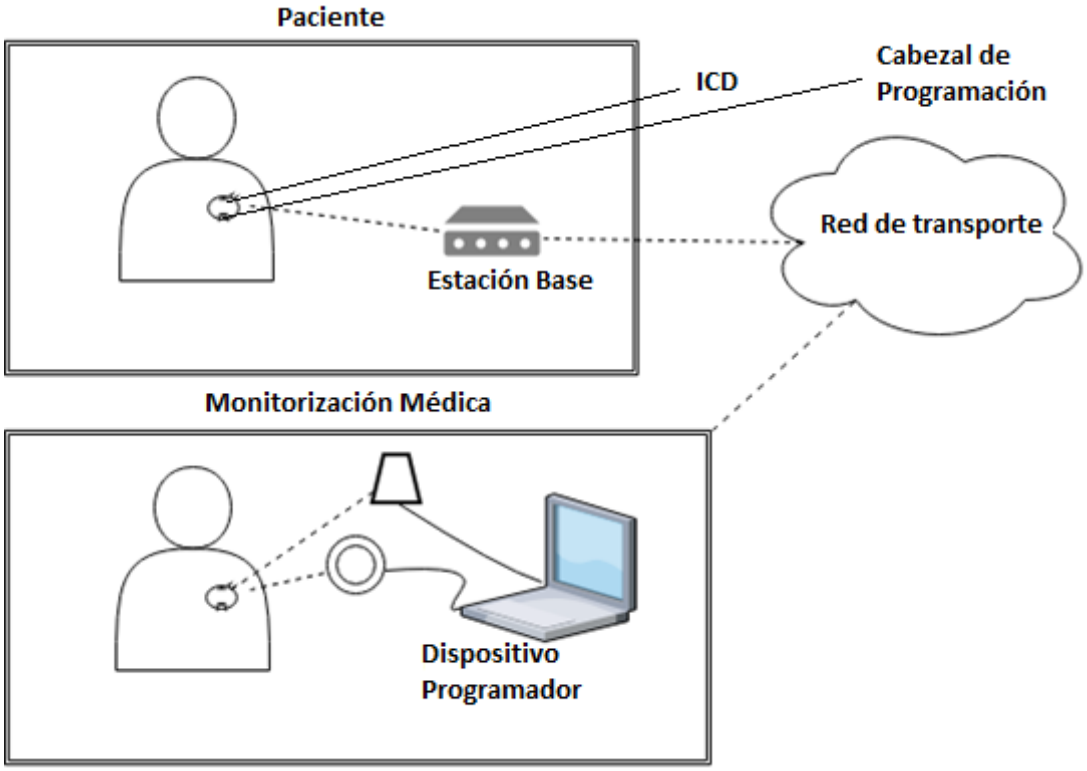


Figura. 2 Arquitectura y funcionamiento del ICD

Se componen de las siguientes partes: [19]

- ICD
- Cabezal de programación
- Dispositivo programador
- Estación Base
- Red de transporte

Dispositivo programador: En otros textos son llamados programador médico, son utilizados por el personal médico para modificar de forma inalámbrica la configuración del ICD.

Estaciones Base: Esta es instalada en el hogar de los pacientes, permiten la supervisión remota mediante la recopilación de los datos de telemetría desde el ICD, así como el envío de estos datos para el hospital.

Cabezal de programación: Está incluido en los dispositivos programados y las estaciones base; se encarga de activar la interfaz inalámbrica del ICD cuando es implantado en el paciente.

Red de transporte: Es una infraestructura de red dedicada que se utiliza para facilitar la transmisión de los datos de la terapia del paciente desde el dispositivo programador a la estación base. [20]

1.7 Estándares

Uno de los estándares es la Comisión Federal de Comunicaciones (FCC) en el año 2000 que no está internacionalmente acordado, de ahí que su uso está restringido con frecuencia en los Estados Unidos solamente.

Las principales normas reguladoras de telemetría para dispositivos médicos son: [21]

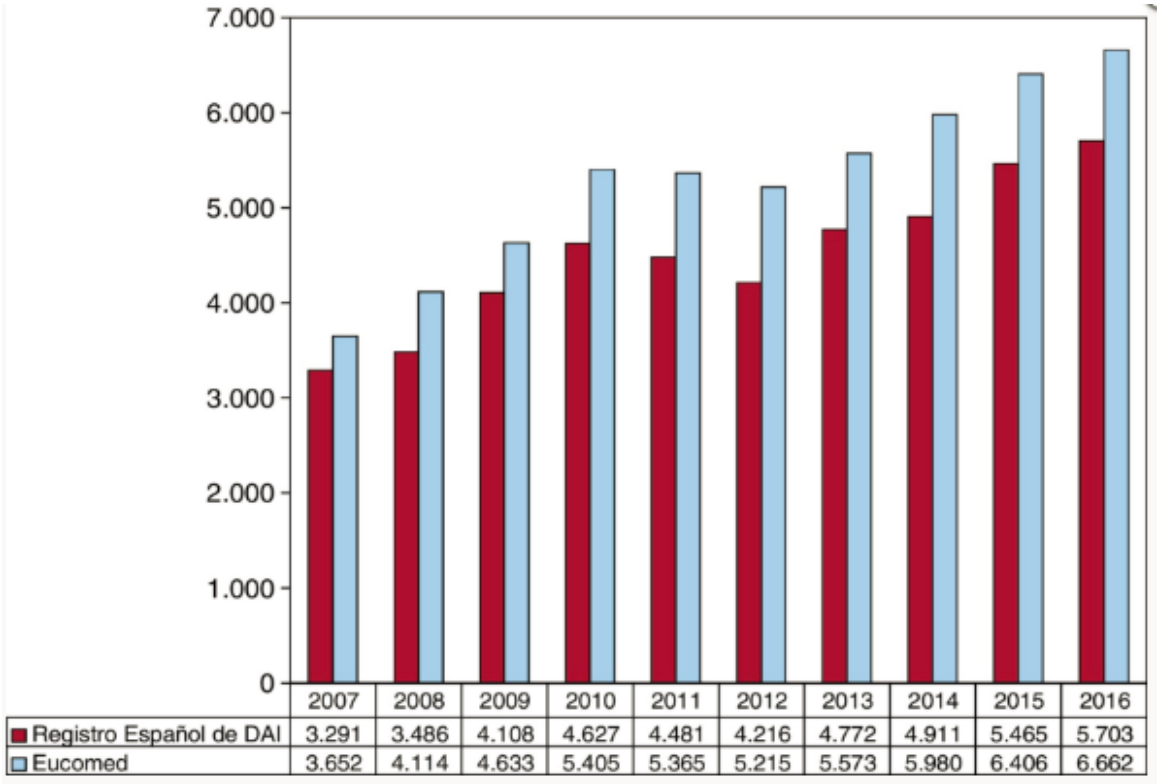
- Servicio de Telemetría Médica Inalámbrica (WMTS): El funcionamiento establece tres bandas de frecuencia: banda de 608-614 MHz, 1395-1400 MHz y 1427-1432 MHz, muchos dispositivos médicos implantables no son compatibles con esta especificación.
- (MICS): Especificación que permite operar a los IMDs bajo el sistema de comunicación de implantes médicos, que opera en la banda de 402-405 MHz. MICS es de baja potencia (25 microvatios), el servicio de radio móvil sin licencia que facilita las comunicaciones de datos entre el IMD y un programador externo. El rango de comunicación es de unos 2 m y el ancho de banda es muy bajo en comparación con tecnologías de comunicación inalámbrica, como Bluetooth o WIFI. Las señales de radio pueden atravesar y transmitirse dentro del cuerpo humano debido a sus características conductivas. El propósito de estas comunicaciones es acceder a las medidas adoptadas por el implante o reconfigurar para, por ejemplo, ajustar el tratamiento. Los MICS IMDs se han proliferado en los últimos años, como los marcapasos, los desfibriladores implantables, neuroestimulador, audífonos y DDSs.
- MedRadio: Es análogo a la especificación WMTS, define los servicios de comunicación tanto para portátiles y dispositivos

médicos implantados. La especificación, que fue aprobada por la FCC en 2009, se extiende la MICS 1 MHz de espectro en ambos lados, cubriendo una banda de frecuencia de 401 a 406 MHz. El uso de estas frecuencias en la IMDs está bien justificado en esas frecuencias, señales de radio puede propagar fácilmente en el cuerpo humano y la banda de 401-406 MHz es compatible con la normativa internacional y no interferir con otras operaciones de radio en la misma banda.

2. Vulnerabilidades

Las vulnerabilidades encontradas en los ICD se relacionan con el uso de mecanismos de autenticación débiles y datos médicos confidenciales sin encriptar o débilmente cifrados.

A continuación, se muestra una gráfica estadística del número de ICDs implantados en España desde el 2007 hasta el 2016.



	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016
Registro Español de DAI	3.291	3.486	4.108	4.627	4.481	4.216	4.772	4.911	5.465	5.703
Eucomed	3.652	4.114	4.633	5.405	5.365	5.215	5.573	5.980	6.406	6.662

Fuente: http://www.revespcardiol.org/es/registro-espanol-desfibrilador-automatico-implantable-/articulo/90461602/ fecha:4-06-2018

Figura. 3 Número total de implantes registrados y los estimados por la European Medical Technology Association (Eucomed) en los años 2007-2016

Se observa que el número total de implantes en 2016 fue 5673, superior al de 2015 que fue 5465. Teniendo en cuenta que, según los datos de Eucomed, el número total de dispositivos fue de 6662, esta cifra representa el 85% del total. [22]

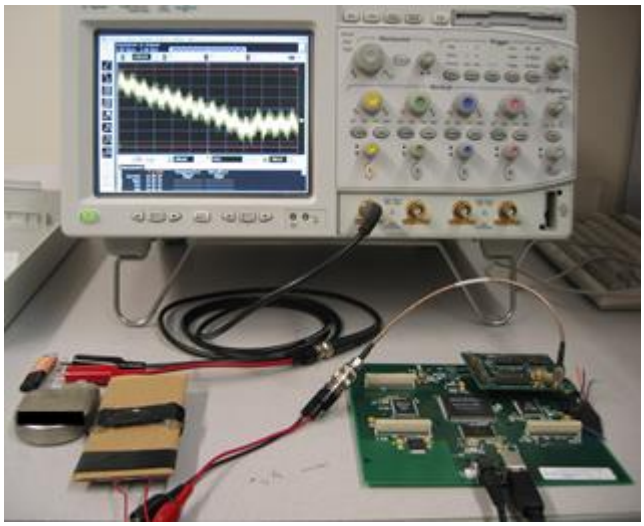
Como se reconoce en la Fig. 3 cada vez son más las pacientes que acceden a este tipo de tratamientos para mejorar su salud, lo cual es preocupante ya que existe una variedad de ataques que podría ser perjudicial para ellos.

2.1 Cronología de vulnerabilidades 2008 al 2018

Año 2008

En el año 2008 se publicó la investigación acerca de los riesgos de seguridad en los ICDs “Ataques de software de radio y defensas de cero potencias” donde se demostraba que la ingeniería inversa en los protocolos de comunicaciones ICD y a través de la creación de ataques de software de radio se comprobó que pueden poner en peligro la seguridad del paciente. Se experimentó en el ICD Medtronic Máximo DR VVEDDDR modelo #7278 (ya no se encuentra disponible en el mercado).

Recreación del ataque de ingeniería inversa



Fuente: https: http://scholarworks.umass.edu/cgi/viewcontent.cgi?article=1067&context=cs_faculty_pubs

Figura. 4 Componentes de ataque de Ingeniería Inversa

Los componentes que se utilizan para este ataque:

En la parte superior hay un osciloscopio de 4 GSa / s.

En la parte inferior, de izquierda a derecha, están:

Una antena de escuchas.

Un ICD,

Una antena transmisora (montada en cartón),

Un USRP con una tarjeta BasicTX adjunta.

Las capturas mediante la “Ingeniería Inversa” encontraron que los datos personales son transferidos en texto plano en el cuál se incluyen el nombre del paciente, número de identificación médica e historial del paciente, nombre y el número de teléfono del médico tratante, fechas de implantación del ICD, el modelo y número de serie del ICD y las derivaciones y otros elementos de datos de identificación personal que se transmiten también en texto plano.

Se puede llegar a la conclusión que el dispositivo programador y el modelo del ICD no protegen sus comunicaciones por lo tanto no utilizan ningún sistema de cifrado.

Año 2010

En el 2010, Maisel y Kohno solicitaron un marco regulatorio específico para la seguridad de dispositivos médicos [23]. Su investigación enfatizó las preocupaciones con las propiedades de seguridad asociadas con los dispositivos que realizan funciones para salvar vidas, como un marcapasos. Además, destacó los riesgos asociados con la arquitectura y las interdependencias de implementación para un ecosistema que se extiende más allá de los riesgos de implementación de los proveedores. También argumentaron que estos dispositivos médicos proporcionan importantes beneficios para la salud de los pacientes y que los controles de seguridad deben balancearse. [20]

Año 2012

En 2012, Burleson y Fu discutieron los desafíos de diseño asociados con la seguridad de los dispositivos médicos implantables [24]. Los autores proporcionaron un modelo de amenaza y discutieron cómo las consideraciones de seguridad importantes se aplican comúnmente en muchos dispositivos cardíacos implantables. Las indicaciones de su investigación muestran subprocesos comunes en varios proveedores de IMD. [20]

Año 2014

Ellouze et al presentaron el trabajo “Investigación de ataques de digitales seguridad en dispositivos médicos implantables cardíacos”. La comunicación del ICD es de forma inalámbrica se comprobó que existen debilidades ya que poseen niveles básicos de autenticación y de cifrado y son vulnerables a ataques detallados a continuación. [25]

Cuando los mensajes intercambiados no están cifrados, el adversario los analiza para descubrir las credenciales y extraer datos sensibles, entre otros incluidos datos fisiológicos proporcionados por el EMG.

Según el análisis de tráfico se constató que los mensajes que se cifran y se protegen con las mismas claves criptográficas y algunos algoritmos de ataques se explotan en modo persistente (por ejemplo, los ataques de fuerza bruta) cuya finalidad es descubrir las credenciales utilizadas para la autenticación, descifrar los comandos intercambiados y configuraciones, afectando la integridad y la confidencialidad del paciente.

En el caso del acceso no autorizado al IMD se obtienen las credenciales utilizadas para la autenticación, un adversario puede autenticarse con éxito al IMD, por lo tanto, tiene acceso a él por completo y obtener los privilegios a entidades autorizadas (por ejemplo, prescripciones médicas). Lo que da como resultado la materialización de algunos ataques que se detallan a continuación y que podrían costarle la vida a un paciente.

- **Generación de descargas eléctricas repetitivas:** Debido al privilegio ganado por el adversario puede inducir al IMD a administrar una serie de descargas eléctricas sucesivas sin la detección de ningún tipo de arritmia.
- **Modificación del registro:** Un atacante puede modificar o eliminar los datos almacenados en los registros. Estos tipos de ataques se usan generalmente para ocultar evidencia que ayuda a los investigadores a identificar un comportamiento normal.
- **Modificación de la terapia:** Un adversario altera la configuración de la terapia o puede llegar a desactivarlo, por lo que el IMD brinda una terapia inapropiada en el futuro.

Atacar la disponibilidad del IMD incluso si un adversario no puede obtener acceso al IMD, puede dañar la disponibilidad del IMD mediante la ejecución de varios tipos de denegación de servicio.

- **Interrupción:** Al interrumpir el tráfico entre el IMD y el dispositivo programador, el médico no podría configurar o actualizar la terapia al IMD mediante el dispositivo programador.
- **Reproducir:** Si los mensajes intercambiados están cifrados, pero son diferentes de una sesión a otra, el atacante puede interceptar mensajes de una sesión y reproducirlos para abrir una nueva sesión como usuario válido o volver a ejecutar los comandos.

Año 2015

En el año 2015 Camara et al desarrollaron la investigación “Las cuestiones de seguridad y privacidad en dispositivos médicos implantables: un estudio exhaustivo”, se ha demostrado que la seguridad de los ICD es bastante limitada, esto recae en tres factores principales:

- Energía
- Almacenamiento
- Comunicación

Energía: Consume la energía, por lo que es de vital importancia el uso correcto de la misma, se podría decir que una seguridad más sólida, una velocidad de transmisión que mayor repercute de forma directa en la batería del dispositivo, sin mencionar que recargar la batería implica una cirugía con las complicaciones que eso abarca.

Para ello se han propuesto varias alternativas que van desde la carga inalámbrica a través de un dispositivo muy cercano al ICD, incluso el aprovechamiento de los movimientos de los músculos para generar energía , de esta forma no sería necesario el reemplazo de la batería, si bien estas son ideas con ventajas y desventajas en algunos aspectos, la realidad nos indica que aún no existe en el mercado comercial una solución a este problema, no al menos algo probado e implementado por lo que los dispositivos actuales aún son vulnerables a ataques para consumir la batería del ICD.

El Almacenamiento: El almacenamiento es muy limitado en estos dispositivos, en donde la mayor parte de la memoria se utiliza para guardar datos de las señales ECG “electrocardiograma” del paciente. La memoria RAM de estos dispositivos va desde 2KB a 36KB para los más antiguos y 128 KB a 1024 KB para lo más nuevos, uno de los aspectos desafiantes para los ICD es el incremento de la memoria, si bien en estos días el tamaño de una memoria puede ser implantado en dispositivos como el ICD, el consumo de energía sería también mayor así que la vida útil de la batería se reduciría.

La comunicación: Un problema en los ICD, ya que las comunicaciones del ICD con el dispositivo externo son muy limitadas debido a que mantener una comunicación es muy costosa en cuestiones de energía, sin mencionar la baja potencia de transmisión que posee el dispositivo.

Solución propuesta

¿Qué se podría hacer al respecto?

En esta investigación se menciona una alternativa utilizada en

algunos dispositivos, y si el ICD no realizará el control de seguridad y si esa función la derivase a otro dispositivo "*Divide et impera" Divide y Vencerás*. Tendría sentido, ya que el consumo de energía sería menor sin mencionar que el dispositivo intermedio podría tener fuertes medidas de seguridad, mayor almacenamiento y una transmisión de datos veloz.

Un ejemplo de ello sería un proxy escudo IMDGuard, cloaker etc. De esta forma no hay una comunicación directa entre el ICD y el dispositivo programador, sino que se comunican a través del proxy, en donde se utiliza un canal cifrado a través del dispositivo externo.

Aunque esta propuesta parece ser ideal presenta también una serie de inconvenientes mencionados a continuación:

Constituye un único punto de falla, por lo cual el malfuncionamiento del mismo, o el hackeo a esta unidad constituye un peligro a la seguridad del paciente, sin mencionar también que se podrían interferir la comunicación entre el dispositivo mediador y el ICD.

Año 2016

Riesgos encontrados en los ICD.

En agosto de 2016, Muddy Waters Research LLC publicó un informe que advertía que los ICD fabricados por St. Jude Medical (ahora Abbott) tenían un alto riesgo de hackeó.

El informe, escrito en colaboración con MedSec (Miami, Florida), una firma de investigación sobre ciberseguridad centrada en la atención médica, detallaba dos tipos de violación de la seguridad de los dispositivos.

La FDA envió una carta de advertencia a Abbott instando a la empresa a aumentar la ciberseguridad basándose en el informe Muddy Waters y la detección de áreas de vulnerabilidad en su sistema de monitoreo remoto.

"Sobre la seguridad de los desfibriladores cardíacos implantables de última generación y cómo protegerlos"

En el 2016, Marin et al explicaron de un ataque por caja negra, en un laboratorio que incluye un USRP, DAQ, y la creación de un receptor con

la ayuda del software LabVIEW, se llegó a deducir el comportamiento de un ICD, el estudio fue efectuado a varios ICDs.

Estos dispositivos operan en una frecuencia de comunicación de corto alcance entre 30-300kHz para la activación del ICD, el dispositivo programador y el ICD se comunican a través de una comunicación de largo alcance 402-405 MHz, la frecuencia de transmisión de los dispositivos médicos puede ser obtenida a través de la FCC, estas frecuencias están destinadas para la comunicación de los implantes médicos.

¿Es posible determinar un comportamiento del ICD solo interceptando las señales de radio?

De hecho, es así porque cuando el ICD está activo la frecuencia con la que se comunica cambia.

Aquí ya empieza a distinguirse un aspecto muy importante, se presenta el siguiente interrogante ¿se puede saber cuándo un ICD está comunicando algo a un dispositivo programador o se envió un mensaje para activarlo?

Se observó que el dispositivo programado y el ICD utilizan modulaciones distintas para transmitir sus datos. La transmisión desde el dispositivo programador al ICD utiliza FSK, DPSK se utiliza en las transmisiones desde el ICD al dispositivo programador. Lo que se comprueba es que el ICD se comunica de una forma con el dispositivo programado y el dispositivo programado con el ICD de una forma diferente.

Para comunicaciones de largo alcance, todos los mensajes tienen en común el inicio de trama o SOF que consiste en una serie de alternancia "1s" y "0s" enviado consecutivamente para indicar la presencia de un mensaje entrante, esto es seguido por un preámbulo que indica que la secuencia de bits de información está a punto de comenzar.

Ahora bien, es evidente que con solo escuchar las señales de radio se puede determinar la dirección del mensaje y diferenciar entre un mensaje de transmisión y la activación de los dispositivos.

Las vulnerabilidades que se pueden hallar desde el análisis de señales, lo cual es preocupante ya que, según el estudio, con materiales accesibles es posible realizar un análisis preciso del comportamiento de los mensajes enviados, analizarlos y obtener conclusiones certeras.

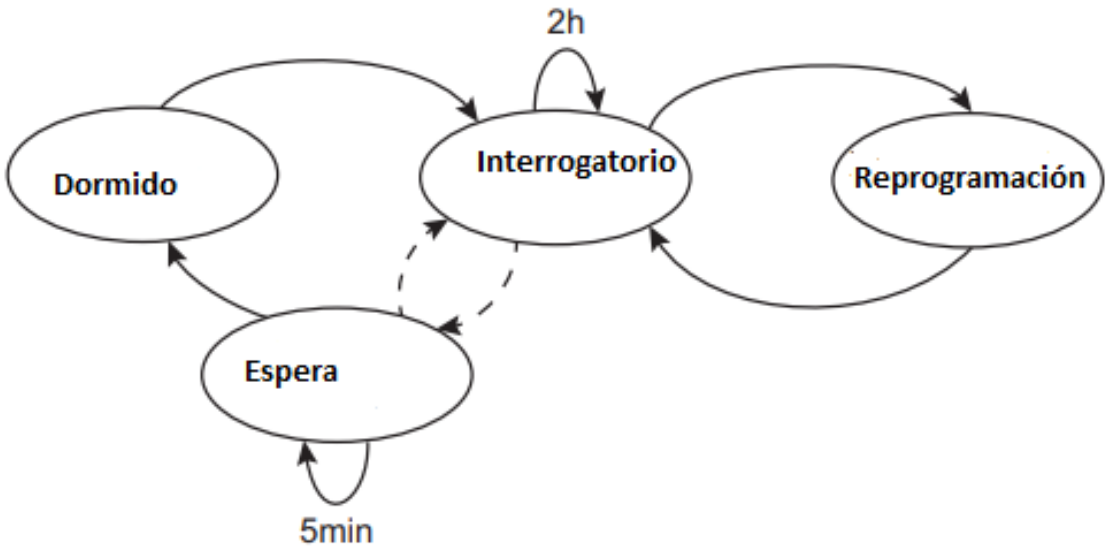
Se logró descifrar los mensajes enviados por el dispositivo programador, se observó una misma secuencia LSFR, lo cual da como resultado un patrón único igual al del modelo ASCII, esto sucede en todos los ICD probados en el experimento.

Los mensajes enviados desde el dispositivo programador al ICD, en este caso cambiar el nombre de paciente, incluye 16 mensajes que siempre está compuestos por dos grupos diferenciados, el primer grupo incluye desde la posición 1 hasta la posición 8 y el segundo grupo del desde la posición 9 hasta el 16 de mensajes.

Cada letra es enviada desde el dispositivo programador al ICD es representado de forma distinta de acuerdo a su posición dentro del nombre del paciente.

En la misma investigación presentó que el ICD opera en 5 estados diferentes:

- Dormido
- Interrogatorio
- Re-programación
- No-telemetría o espera



Fuente: https://www.esat.kuleuven.be/cosic/publications/article-2678.pdf
Figura. 5 Modos de operación del ICD

Uno de los modos en donde se puede explotar vulnerabilidades es el modo de espera y dormido.

- En este modo se podría secuestrar una sesión y enviar comandos maliciosos.

Si está en modo espera, cualquier dispositivo programador puede activar de nuevo el ICD enviando un mensaje específico sobre el canal de comunicación de largo alcance. Este mensaje es idéntico para todos los ICDs, y mantiene activo al ICD consumiendo más rápidamente su batería o abriendo una ventana más larga de comunicación para enviar comandos maliciosos.

Como la investigación lo demuestra, el hacker podía interceptar las señales del ICD con el dispositivo programador y capturarlos, de esta forma podría realizar un ataque a la persona desde una mochila en un autobús, cargando en ella todos los dispositivos necesarios para el ataque.

Esto sin duda muestra que una seguridad por obscuridad si no es bien aplicada es muy vulnerable por lo que es recomendable utilizar los estándares de seguridad para las comunicaciones.

Lo más preocupante de la situación es que los ataques pueden ser realizados con aparatos que se pueden conseguir en una tienda de electrónica, incluso se podría adquirir aparatos legítimos para realizar

ataques.

Un tipo de ataque mencionado también es a través de dispositivos legítimos, ya que se demostró que cualquier estación base del ICD puede activar el ICD, en donde el ICD permanece en modo de espera lo cual se podría explotar la vulnerabilidad por modo de espera mencionado anteriormente.

Existe también un aspecto a mencionar, no siempre es necesario estar muy cerca del paciente para llevar un ataque también es posible aumentar la distancia de la comunicación a través de equipos sofisticados y antenas direccionales, por lo cual el ataque podría ser a una mayor distancia.

La privacidad de los datos está seriamente comprometida, porque es posible a través del espionaje del canal inalámbrico, en donde los datos privados del paciente y datos de su telemetría sean monitoreados ya que se notó que los datos enviados por vía aérea son ofuscados utilizando la misma secuencia LFSR mencionado anteriormente.

La denegación de servicio es otra vulnerabilidad encontrada, se realiza cuando la sesión de conexión del dispositivo ICD caduca, es posible cambiarla a modo interrogatorio enviando un mensaje desde el dispositivo malicioso de largo alcance, este mensaje es igual para todos los ICD, por lo cual se podría agotar la batería del dispositivo de forma más rápida, sin mencionar que se podría extender la ventana de comunicación el tiempo que se desea.

Del mismo modo son susceptibles a los ataques de suplantación y reproducción a través del envío de mensajes anteriores, ya que el protocolo de comunicación no posee ningún medio para verificar la integridad y autenticidad de los mensajes.

Un aspecto importante es que el ICD debe responder incluso si la autenticación falla, lo que supondría un consumo de batería extra por cada respuesta.

¿Qué dificultades se encuentran en estos dispositivos?, ¿Porque

no se agrega una mayor seguridad? Si bien se podría suponer que la agregación de un cifrado más sólida basada en claves simétricas y una distribución de las mismas por ejemplo por DIFFIE- HELLMAN proporcionaría una mayor seguridad, o incluso el aumento de la potencia de comunicación daría una mejor respuesta a las situaciones más críticas en donde el tiempo de respuesta es algo crítico, pero se halla con ciertas limitaciones tanto físicas, como de accesibilidad del dispositivo.

Año 2017

WhiteScope realizó una evaluación de seguridad exhaustiva en el ecosistema de dispositivos cardíacos implantables en el cuál ha utilizado programadores médicos, dispositivos de monitoreo en el hogar y dispositivos cardíacos implantables para cuatro principales proveedores de dispositivos cardíacos implantables. Conceptualmente los cuatro proveedores principales emplean un marco de arquitectura similar, que incluye protocolos de comunicación, intercomunicaciones de dispositivos, hardware de dispositivos integrados y autenticación de dispositivos. El análisis reveló riesgos de seguridad potenciales derivados de los protocolos subyacentes y las comunicaciones de sistema a sistema que involucran dispositivos integrados.

Algunas vulnerabilidades encontradas: [20]

Mapa De La Imagen De Firmware En Memoria Protegida

La asignación de la imagen del firmware a la memoria protegida evita la capacidad de sobrescribir o alterar la funcionalidad crítica del subsistema mientras el subsistema está funcionando. Si la imagen del firmware se asigna a la memoria protegida, el atacante debe usar un área de memoria diferente para cargar código malicioso. Los dispositivos de monitoreo en el hogar carecían de un esquema de implementación que incorpora el mapeo de imágenes de firmware en la memoria protegida. Como resultado, un atacante tiene el poder de escribir comandos arbitrarios en la memoria y alterar la funcionalidad del sistema central.

Conexiones Externas USB

Los dispositivos de monitoreo en el hogar incluyen conexiones USB externas que permitían comunicaciones a nivel de sistema. Al aprovechar las conexiones USB, un atacante puede atravesar el sistema de archivos o introducir software malicioso en los dispositivos de monitoreo del hogar. Aunque se requiere para algunas funciones del sistema, las conexiones USB deben estar bloqueadas de tal manera que permitan sólo los dispositivos autorizados.

Datos Credenciales e Infraestructuras en Código

Los dispositivos embebidos a menudo utilizan esquemas de autenticación de dispositivo a dispositivo. Como consecuencia, las credenciales para la autenticación deben almacenarse de alguna manera en el sistema de autenticación. El análisis reveló el uso de credenciales codificadas en los dispositivos de monitoreo en el hogar para autenticarse en las redes de asistencia al paciente. En tres vendedores, se obtuvieron valores de texto plano. Como resultado, un atacante usa las credenciales para autenticarse en la red de asistencia al paciente. Al igual que las credenciales codificadas, los datos de infraestructura codificados a menudo se usan en las comunicaciones de dispositivo a dispositivo. Se implementaron datos de infraestructura codificados en los dispositivos de monitoreo del hogar para facilitar la comunicación con las redes de asistencia al paciente. Los datos de infraestructura incluyeron números de teléfono y direcciones IP que corresponden a servidores de autenticación para la red de asistencia al paciente. Como resultado, un atacante puede identificar los servidores de autenticación para la red de asistencia al paciente. Debido a la naturaleza sensible de las credenciales codificadas y los datos de infraestructura, estas herramientas se han eliminado de este informe.

Actualización de Firmware Remoto

Los dispositivos de monitoreo en el hogar reciben actualizaciones de firmware a través de la red de asistencia al paciente. Sin embargo, los dispositivos de monitoreo en el hogar no necesariamente validan la fuente del sistema que distribuye el firmware. Como resultado, existe la posibilidad

de realizar un ataque de intermediario y emitir firmware falsificado a un dispositivo de monitoreo doméstico.

Firmware Digitalmente Firmado

El firmware firmado digitalmente garantiza que un dispositivo solo que ejecutará el firmware autorizado, incluso si se recibe de una entidad no autorizada. Sin embargo, el firmware firmado digitalmente no se implementó para subsistemas dentro del ecosistema de dispositivos cardíacos implantables. Como resultado, existe la posibilidad de cargar y ejecutar firmware falsificado en un dispositivo de monitoreo doméstico.

Medios de comunicación extraíbles / discos duros

Los programadores médicos utilizan medios extraíbles / discos duros. Como resultado, un atacante tiene el potencial de montar los medios extraíbles y extraer todo el sistema de archivos para los programadores médicos.

Uso de Bibliotecas de Terceros

Los desarrolladores de software aprovechan los componentes de terceros (por ejemplo, las bibliotecas) para ayudar a acelerar el proceso de desarrollo. Sin embargo, la inclusión de componentes de terceros puede introducir vulnerabilidades potenciales que a menudo quedan sin parchear.

El análisis de los programadores médicos mostró la inclusión de componentes de terceros. Además, varias instancias incorporaron componentes de terceros obsoletos y vulnerables. Como resultado, puede existir la posibilidad que un atacante aproveche las explotaciones públicamente conocidas para comprometer el subsistema. Los números relacionados con el uso de componentes de terceros identificados y el número asociado de vulnerabilidades conocidas para los programadores médicos se enumeran a continuación.

	Vendedor Uno	**Vendedor Dos**	**Vendedor Tres**	**Vendedor Cuatro**

Número de componentes de terceros identificados	201	47	77	21
Número de componentes de terceros vulnerables	74	39	51	10
Número identificado de vulnerabilidades conocidas en componentes de terceros	2.354	3.715	1.954	642

Año 2018

Adrián Baranchuk y un grupo de sus colaboradores han publicado recientemente en el JACC un texto de la ciberseguridad para los dispositivos electrónicos implantables de uso común en Cardiología*. [26]

Señalan los autores que los dispositivos médicos han sido objeto de piratería durante más de una década, y este problema de la ciberseguridad ha afectado a muchos tipos de dispositivos médicos.

Últimamente, el potencial de la piratería ha afectado a dispositivos cardíacos (marcapasos y desfibriladores) lo que fue objeto de atención de los medios de comunicación y de preocupación para los pacientes y los proveedores de atención médica.

Este es un problema creciente del nuevo mundo conectado electrónicamente. En este documento el Consejo de la Sección de Electrofisiología del Colegio Americano de Cardiología, discuten brevemente varios aspectos de esta amenaza relativamente nueva, que se relacionan a recientes incidentes que involucraron a los dispositivos cardíacos implantables

Se exploran también los posibles riesgos para los pacientes y el efecto que pueda tener la reconfiguración de los dispositivos en un intento de frustrar las amenazas a la seguridad, se proporciona un resumen de lo

que se puede hacer para mejorar la ciberseguridad desde el punto de vista del fabricante, el gobierno, las sociedades profesionales, el médico y el paciente.

La piratería

La piratería o hackeó se define como el acceso no autorizado a un sistema informático para obtener información o crear problemas dentro del sistema.

En la actualidad, los piratas informáticos o hackers se han entrometido en la mayoría de las áreas factibles. Una búsqueda en Google de “piratería informática [dispositivos como refrigeradores, monitores para bebés, televisores]” proporciona múltiples resultados interesantes y / o preocupantes.

La ciberseguridad

La verdadera ciberseguridad comienza cuando se diseña un software protegido desde el principio, y requiere la integración de múltiples partes interesadas, incluidos expertos en software, expertos en seguridad y asesores médicos.

El creciente número de dispositivos médicos que usan software ha creado una nueva preocupación de seguridad cibernética en la industria médica: ¿Cómo podemos proteger y garantizar su funcionamiento normal a los dispositivos de la interferencia dañina intencional?

Las comunicaciones inalámbricas avanzadas entre los proveedores de atención médica y los dispositivos de los pacientes han creado la posibilidad de manipular las interacciones normales, incluidas las funciones de desactivación; retrasar, interferir o interrumpir las comunicaciones; y alterando la programación.

Esto plantea un riesgo potencial para la atención clínica, ya que los pacientes podrían verse perjudicados por la acción de un cambio nocivo, inadvertido o maligno, en la programación de los “hackers”.

Los problemas de seguridad del paciente con respecto a los marcapasos se limitan en gran medida a la activación mal intencionada del ICD lo cual produce el potencial agotamiento de la batería.

Como ocurre con otras causas de interferencia electromagnética (radioterapia, electrocauterización y soldadura), la detección de señales de origen no cardiaco puede inhibir la estimulación, induciendo períodos prolongados de asistolia con el consiguiente riesgo de síncope o muerte súbita. El agotamiento repentino de la batería también es clínicamente más relevante en un paciente dependiente del ritmo.

Las mismas áreas de vulnerabilidad en los marcapasos también se aplican a los desfibriladores cardiacos implantables.

La interrupción de las comunicaciones inalámbricas (monitoreo remoto) sería posible para un pirata informático que opera en la misma radiofrecuencia que el dispositivo médico, y la interrupción de la comunicación inhibiría el valor de la tele monitorización y permitiría que el sistema no detectara ningún evento clínicamente relevante.

En un paciente dependiente de estimulación con un desfibrilador cardiaco implantable, la sobre detección puede inhibir la estimulación.

Además, la sobre detección puede resultar en descargas inapropiadas e incluso potencialmente mortales. Si se realizara la reprogramación, las terapias de desactivación (estimulación anti taquicardia y descargas) no darían como resultado la respuesta del dispositivo a las taquicardias ventriculares que amenazan la vida.

Inducir arritmias a través de estimulación no invasiva programada también podría ser un riesgo potencial. El agotamiento repentino de la batería sigue siendo una preocupación clínica en los pacientes que dependen del ritmo cardíaco debido a la incapacidad para administrar terapias durante las arritmias clínicas que amenazan la vida.

Un enfoque seguro del ciclo de vida del sistema comienza en la concepción del desarrollo del dispositivo y continúa a través de la fabricación y la monitorización posterior al implante.

Las necesidades de ciberseguridad también deben abordarse durante las pruebas de productos previas y posteriores al mercado. Dado que las vulnerabilidades cibernéticas pueden surgir rápidamente, se deben implementar procesos sólidos de post-comercialización para monitorear el entorno en busca de nuevas vulnerabilidades y responder de manera oportuna.

En dispositivos de generación actual que tienen vulnerabilidades teóricas o conocidas, el firmware (definido como un tipo de software que está integrado en el hardware de un dispositivo tecnológico que requiere actualizaciones de vez en cuando) es útil.

Es posible monitorear o interrogar remotamente a todos los dispositivos con tele monitorización, ya que todos los ICD que se están siguiendo de forma remota ya se comunican con el sitio web del fabricante.

En este momento, no hay evidencia de que uno pueda reprogramar un ICD o cambiar la configuración del dispositivo de ninguna forma. La probabilidad de que un pirata informático individual afecte con éxito a un ICD o sea capaz de dirigirse a un paciente específico es baja. Un escenario más probable es el de un ataque de malware o ransomware que afecte a la red de un hospital e impida la comunicación.

En este caso, la pérdida de la comunicación remota puede evitar la transmisión oportuna de un evento clínico. Si se produce esta situación, es posible que se requiera una cita en persona para restablecer la comunicación con el dispositivo y el paciente; esto puede no ser conveniente para pacientes que viven en lugares remotos.

Hasta el momento, no ha habido informes clínicos reales de piratería maliciosa o inadvertida o ataques de malware que afecten a los ICD. La mayoría cree que el riesgo teórico de una violación a la seguridad cibernética está muy por encima del riesgo de la actualización del software.

Basado en la investigación de modos de falla, este no es un problema restringido a Abbott. Existen riesgos para cualquier dispositivo que esté conectado a Internet. Fuera del ámbito de la gestión ICD, estos problemas obviamente también se aplican a otros dispositivos médicos (bombas para el dolor, bombas de insulina, presión positiva continua en las vías respiratorias y monitorización de ritmo y hemodinámica) que están conectados a Internet para monitorización y programación remota.

Los médicos que manejan los ICD deben conocer los riesgos documentados y posibles de ciberseguridad. Se deben establecer sistemas para comunicar las actualizaciones en estas áreas de forma rápida y comprensible para el resto del equipo clínico que maneja pacientes con dispositivos.

Las políticas y los procedimientos para estas comunicaciones pueden ser informados por la respuesta previa de la clínica a los retiros de dispositivos de la FDA. Hay una variedad de recursos disponibles a través de Abbott abordando específicamente el tema de ciberseguridad en su comunicado de prensa y su sitio web.

Las clínicas y los hospitales deben revisar las actualizaciones de seguridad y estar al tanto de los problemas que se presentan. Los pacientes deben participar en la conversación, y una decisión compartida es fundamental. En este momento, el Consejo de Electrofisiología considera que no es necesario un monitoreo mejorado o el reemplazo de un dispositivo electivo. El efecto general del firmware aún no se ha entendido.

No todos los ICD son iguales, y el resultado potencial de la piratería depende tanto del tipo de dispositivo como de la dependencia del paciente. Cuantas menos interacciones remotas con un dispositivo, existen menos posibilidades de que los hackers interrumpan las comunicaciones.

Sin embargo, dada la falta de evidencia de que el hackeó sea un problema clínico relevante, junto con la evidencia de los beneficios del monitoreo remoto, se debe tener precaución al privar al paciente del beneficio claro de la monitorización remota.

El posible efecto futuro de este problema es inmenso. La FDA, los fabricantes y las sociedades profesionales como el Colegio Americano de Cardiología y la Sociedad del Ritmo Cardíaco participan activamente en conversaciones más amplias sobre los riesgos generales y la mejor forma de proteger a los pacientes y proporcionar la atención más efectiva.

Esta es un área en evolución de atención médica y regulación legal, que continuará progresando rápidamente. Todos deberíamos estar atentos.

Alternativas para mitigar el riesgo

Después de exponer las vulnerabilidades a lo largo de los últimos 10 años en los ICD. Algunos grupos de investigadores han expuesto posibles soluciones para mitigar el riesgo.

En la investigación “Sobre la seguridad de los desfibriladores cardíacos implantables de última generación y cómo protegerlos” en donde se indican medidas de corto y largo plazo.

A corto plazo

Una de las soluciones propuestas es a través de la aplicación del comando "shutdown" en los dispositivos externos, para que el canal inalámbrico quede bloqueado mientras esté en modo de espera o si un atacante es identificado bloquear la conexión de forma inmediata, como desventaja se presenta que una persona podría bloquear la conexión de un dispositivo legítimo aunque por lo general la conexión del ICD con el dispositivo externo se hace en un hospital o en una casa lo cual en cierta forma limita esta posibilidad.

A largo plazo

Incluye el mensaje de apagado tanto en el ICD como en el dispositivo externo, de esta forma el dispositivo externo puede enviar un mensaje de parada al ICD para que pase en modo apagado.

Una forma interesante de encarar una solución es a través de las situaciones que pueden presentarse, es decir ¿Cómo debería actuar de

forma normal y como en una situación de emergencia? De acuerdo a la investigación “Las cuestiones de seguridad y privacidad en dispositivos médicos implantables: un estudio exhaustivo.” Nos describe algunas alternativas:

Seguridad en modo normal de operación

El paciente controla qué entidad puede actuar con su ICD, en este caso el mecanismo de autenticación y protocolos de cifrado deben ser bastantes sólidos, debería ser indetectable ante usuarios no autorizados.

Aunque se plantea la siguiente situación, ¿qué pasaría si un paciente debe ser intervenido de forma urgente en un hospital en que no posee acceso a su ICD?

Modo de emergencia

Aquí la seguridad del dispositivo se vuelve un riesgo potencial para el paciente ya que los médicos no podrían reprogramar el dispositivo para una medida urgente, aquí el estudio plantea que el ICD debe poseer un modo de emergencia en donde el ICD debería brindar información acerca del tratamiento aplicado, su modelo, marca y su desactivación en caso de una cirugía de emergencia.

IV. Propuesta por parte del autor

En una opinión personal, se ha pensado que una integración de posicionamiento del paciente podría tomarse como un parámetro de autenticación, es decir al iniciar la conexión con el ICD, se podría verificar si el paciente está realmente en un hospital o algún otro lugar donde el ICD por ende pueda ser accedido, si bien esto también facilita al atacante realizar un ataque en el hospital sería más limitado su rango de ataque, de forma a salvar la vida del paciente si el ataque es realizado en una institución médica, por supuesto que la verificación de posicionamiento solo se realizaría una vez validado una clave de acceso previa, esto para optimizar el consumo de energía que como se ha visto es un factor muy limitante en estos dispositivos, una desventaja de esto sería realmente que el paciente debería de estar en un hospital para acceder a un ICD.

Lo que se propone es la estandarización única de los ICDs lo que es preocupante, si una persona posee una emergencia lo primero que los médicos deberán conocer qué tipo de implante posee, lo cual no siempre es obvio, incluso el paciente puede desconocer la marca del ICD, esta incompatibilidad tecnológica podría ser fatal para el paciente.

Se deberían diseñar mecanismos de seguridad en la transmisión de los ICDs al dispositivo programador, sin afectar el rendimiento del mismo. Esto sería desde el punto de vista de hardware.

V. Conclusiones

Con la necesidad de mejorar la salud de las personas en afecciones cardiacas se crearon los ICDs lo cual trajo muchas ventajas, pero con el avance de la tecnología también surgieron nuevas amenazas que pueden llegar a quitarles la vida.

El problema real de estos ICD se hace peor si con ella va la ingeniería social, es decir si sabemos por dónde frecuenta una persona, que lugares visita y el tiempo aproximado, se podría realizar los ataques de forma frecuente, o incluso se podría ir probando posibilidades hasta vulnerar la seguridad del dispositivo, ya que como se ha visto la seguridad por oscuridad no es muy efectiva en estos dispositivos.

Se expuso una variedad de vulnerabilidades que han sido comprobados en ensayos en el que fue basado este trabajo, la mayoría realizados en Europa y EEUU, pero ni uno ha sido elaborado acá en América Latina, es preocupante ya que existen pacientes que se benefician de estos dispositivos sin saber a los peligros que están expuestos.

Si bien se ha visto la evolución del ICD en los últimos 10 años, resulta aún escasa y la tranquilidad que las personas con estos implantes puedan tener. En definitiva, un dispositivo con conectividad a un órgano humano no puede ser tratado meramente como un simple programa de computadora, debe enfocarse ya a un nivel de ciberseguridad elevando el nivel de los estándares de seguridad actualmente existentes.

VI. Referencias

[1] D. Fernandéz Sánchez, Diseño lógico de una aplicación para determinar el nivel de seguridad de un dispositivo IoT, 2017.

[2] «Definicion ABC,» 2007-2017. [En línea]. Available: https://www.definicionabc.com/comunicacion/antena.php. [Último acceso: 20 11 2017].

[3] «Clinica de la Universidad de Navarra : Diccionario Médico,» [En línea]. Available: https://www.cun.es/diccionario-medico/terminos/asistolia. [Último acceso: 29 10 2018].

[4] «¿Qué es una bomba de insulina?,» Medtronic, [En línea]. Available: http://www.medtronicdiabeteslatino.com/productos/bombas-de-insulina/que-es-una-bomba-de-insulina. [Último acceso: 2 11 2018].

[5] E. Magaña Lizorrondo, E. Izkue Mendi, M. Prieto Miguez y J. Villandangos Alonso, «Comunicaciones y redes de computadores: problemas y ejercicios resueltos,» de *Problemas y ejercicios resueltos*, Madrid, 2003, p. 216.

[6] «AboutKidsHealth,» [En línea]. Available: https://www.aboutkidshealth.ca/Article?contentid=1278&language=Spanish. [Último acceso: 29 10 2018].

[7] «Significados,» [En línea]. Available: https://www.significados.com/osciloscopio/. [Último acceso: 20 11 2017].

[8] 20 11 2017. [En línea]. Available: https://securityhacklabs.blogspot.com.ar/2017/05/que-es-gnu-radio.html.

[9] B. Perez Titos y O. Ramos, «MEDWave,» 04 2004. [En línea]. Available: https://www.medwave.cl/link.cgi/Medwave/Enfermeria/Mar2004/2714. [Último acceso: 20 11 2017].

[10] M. Callejon, D. Naranjo Hernandez, J. Reina Tosina y L. Roa, «A Comprehensive Study Into Intrabody Communication Measurements,» *IEEE Transactions on Instrumentation and Measurement,* nº 9, pp. 2446-2455, 15 05 2013.

[11] M. Callejon, L. Roa, J. Reina-Tosina y D. Naranjo-Hernandez, «Study of Attenuation and Dispersion Through the Skin in Intrabody Communications Systems,» vol. 16, nº 1, pp. 159-165, 1 2012.

[12] A. Brucker y H. Petritsch, «Extending access control models with break-glass,» pp. 197-206, 2009.

[13] «Cardiolatina Comunidad Iberoaméricana de Cardiología,» 23 02 2018. [En línea]. Available: http://cardiolatina.com/noticias/ciberseguridad-para-los-dispositivos-electronicos-implantables-de-uso-comun-en-cardiologia/. [Último acceso: 22 10 2018].

[14] K. V. Brown, «Existen miles de fallos técnicos que convierten en vulnerables a los marcapasos frente a los hackers,» 28 5 2017. [En línea]. Available: https://es.gizmodo.com/existen-miles-de-fallos-tecnicos-que-convierten-en-vuln-1795618634. [Último acceso: 17 05 2018].

[15] H. Chi, L. Wu, X. Du, Q. Zeng y P. Ratazzi, *e-SAFE: Secure, Efficient and Forensics-Enabled Access to Implantable Medical Devices,* 6 04 2018.

[16] M. d. C. Francés Díez, E. Sanchez Revilla y M. De la Her Díez, «Evolución y perspectiva actual del desfibrilador automático implantable,» pp. 187-188.

[17] «Implantable Cardioverter Defibrillaton (ICD),» Harvard Health Publishing, Harvard Medical School, 06 2014. [En línea]. Available: https://www.health.harvard.edu/heart-health/implantable-cardioverter-defibrillator-icd-. [Último acceso: 22 05 2018].

[18] R. Simons, F. Miranda y D. Hall, Rf telheidu2011emetry system for an implantable bio-mens, in: IEEE MIT-S International Microwave Symposium Digest, 2004, pp. 1433-1436.

[19] E. Marin y et al, «"On the (in) security of the Latest Generation Implantable Cardiac Defibrillators and How to Secure Them",» *ACM,* 05 09 2016.

[20] B. Ríos y J. Butts, *Security Evaluation of the Implantable Cardiac Device Ecosystem Architecture and Implementation Interdependencies,* p. 27, 17 05 2017.

[21] J. Tapiador, C. Camara y P. Peris, «Security and Privacy Issues in Implantable,» *Journal of Biomedical Informatics,* p. 47, 04 2015.

[22] J. Alzueta y I. Fernandez - Lozano, «Revista Española de Cardiología,» 11 11 2017. [En línea]. Available: http://www.revespcardiol.org/es/registro-espanol-desfibrilador-automatico-implantable-/articulo/90461602/#f0010. [Último acceso: 04 06 2018].

[23] W. H. Maisel y K. Tadayoshi, *Improving the Security and Privacy,* vol. 362(13), pp. 1164-1166, 2010.

[24] W. Burleson, C. Shane S, B. Ransford y K. Fu, *Design Challenges for Secure Implantable Medical Devices,* 3-7 06 2012.

[25] N. Ellouge, S. Rekhis, A. Mohamed y N. Boudriga, *Digital Investigation of Security Attacks on Cardiac Implantable Medical Devices,* pp. 15-30, 2014.

[26] «Ciberseguridad para los dispositivos electrónicos implantables de uso común en Cardiología,» 17 02 2018. [En línea]. Available: http://cardiolatina.com/noticias/ciberseguridad-para-los-dispositivos-electronicos-implantables-de-uso-comun-en-cardiologia/. [Último acceso: 2018 10 22].

[27] D. Halperin y et al, «Pacemakers and Implantable Cardiac Defibrillators:Software Radio Attacks and Zero-Power Defenses,» *IEEE,* 2008.

[28] J. A. Hansen y N. M. Hansen, «"A Taxonomy of Vulnerabilities in",» 8 10 2010.

[29] E. Marin, F. D. Garcia, T. Chothia, R. Willems, D. Singelée y B. Preneel, «On the (in)security of the Latest Generation Implantable,» 05 09 2016.

[30] J. Webster, «Desing of Cardiac Pacemakers,» *IEEE Press,* 1995.

[31] B. Wayne, S. Shane , B. Ransford y K. Fu, «Design Challenges for Secure Implantable Medical Devices,» p. 6, 3-7 6 2012.

VII. Índice de Figuras