Política y tecnología de la salud 10 (2021) 100549

Listas de contenidos disponibles en ScienceDirect

Política y tecnología de salud

revista Página de inicio: www.elsevier.com/locate/hlpt

Artículo de revisión

Ciberseguridad en la Internet de las cosas médicas

Nicole M. Thomasian *, Eli Y. Adashi

The Warren Alpert Medical School, Brown University, Providence, RI, Estados Unidos

INFORMACIÓN DEL ARTÍCULO

Palabras clave:

La seguridad cibernética

Internet de las Cosas

Preparación para la salud pública

Política de salud

ABSTRACTO

Fondo: El Internet de las cosas ha generado una nueva flota de dispositivos médicos repletos de capacidades mejoradas de detección y activación. La mitigación preventiva de los riesgos cibernéticos que surgen en este espacio hiperconectado es necesaria para garantizar la seguridad continua del paciente.

Objetivo: El objetivo de este documento es analizar la solidez de las medidas de política existentes para asegurar las tecnologías de Internet de las cosas médicas. El ecosistema regulatorio en los EE. UU. Se analiza principalmente en este documento e incluye marcos regulatorios para la industria, asociaciones público-privadas e iniciativas de transparencia.

Métodos: Se realizó una revisión cualitativa de la literatura médica sobre ciberseguridad con la recopilación de documentos legales federales e internacionales, informes de políticas, marcos de la industria, análisis de violaciones cibernéticas y artículos de revistas científicas.

Resultados: Los documentos de orientación regulatoria presentados hasta la fecha que abordan la ciberseguridad en Internet of Medical Things ponen un énfasis clave en la identificación de dispositivos, la administración de dispositivos heredados, la seguridad física mejorada y la detección de infracciones. Las tendencias de supervisión recientes apuntan a reforzar la autoridad federal en torno a la aplicación de salvaguardas de seguridad de base.

Conclusiones: Se necesita orientación regulatoria adicional para mitigar los riesgos en los dispositivos de Internet de las cosas médicas conferidos por las infraestructuras de TI modernizadas, las interfaces de borde a la nube y los componentes de dispositivos listos para usar. Los avances recientes en el ámbito cibernético también plantean la posibilidad de nuevos vectores de ataque, sistemas ciberfísicos autónomos y amenazas de computación cuántica. Las intervenciones para promover la conciencia y la higiene de la seguridad en torno a los dispositivos de Internet de las cosas médicas pueden empoderar a los usuarios finales y facilitar una respuesta a incidentes sin problemas.

Resumen de Lay: El auge de las tecnologías "inteligentes", como los asistentes de voz y los electrodomésticos adaptables para el hogar, nos acerca a un mundo más personalizado que puede mejorar nuestra vida diaria. El campo de la medicina cambiará con estas tecnologías de "Internet de las cosas" de próxima generación que poseen la capacidad de interactuar con sus usuarios y el entorno que les rodea. Estas tecnologías son importantes porque la precisión con la que los dispositivos médicos interactúan con los pacientes, los trabajadores de la salud y otras tecnologías pueden tener un gran impacto en la atención del paciente. A pesar de toda su promesa, la mayor interconectividad que poseen estos dispositivos también confiere riesgos de ciberseguridad adicionales. La regulación de las políticas y la preparación para la salud pública son fundamentales para garantizar que los beneficios de estas tecnologías emergentes no se produzcan a expensas de la seguridad y la privacidad del paciente. En esta revisión,

Introducción

El grado en el que los dispositivos pueden interactuar de manera óptima con los pacientes, los proveedores de atención médica y otras tecnologías puede afectar significativamente la prestación de atención. En una transición que refleja la industria en general, los dispositivos médicos ahora a menudo aprovechan las redes que pueden ofrecer comunicaciones mejoradas, seguridad y control de retroalimentación. De hecho, la tecnología médica se ha asegurado un lugar entre la Internet de las cosas (IoT) en el cuerpo cada vez mayor de dispositivos integrados que automatizan nuestro mundo. Pero esta revolución digital no es solo de escala sino también de proximidad. Lo que una vez fue una red de dispositivos ahora es una red de dispositivos humanos. A pesar de todo su atractivo, este reciente impulso a la interconectividad también confiere riesgos de seguridad adicionales. Un solo punto débil en estas redes enrevesadas podría muy bien paralizar la infraestructura de salud vital. Es más, con los humanos directamente en el circuito, los riesgos del subterfugio cibernético son más altos que nunca. Los riesgos se complican aún más por el terreno cambiante

* Autor correspondiente.

Dirección de correo electrónico: nicole_thomasian@brown.edu (NM Thomasian).

https://doi.org/10.1016/j.hlpt.2021.100549

On-line el 4 de julio de 2021

debajo. La nueva tecnología se presta a nuevos objetivos, lo que implica la necesidad de sistemas ágiles de ciberseguridad que puedan combatir estas amenazas emergentes en tiempo real.

Más que técnicamente factible, el desmontaje generalizado de dispositivos médicos es una amenaza inminente [1]. Las recientes campañas de malware en hospitales han demostrado claramente que los datos sanitarios ya están siendo atacados a nivel mundial.[2]. No hay nada que impida que sucedan eventos similares en el contexto de los dispositivos médicos. Es en este contexto en evolución que evaluamos el panorama de ciberamenazas existente. Es de destacar que el alcance del término "dispositivo médico" es amplio y se refiere en general a elementos utilizados para la prevención, el diagnóstico, el tratamiento o la cura de enfermedades (consultetabla 1). Nos enfocamos en la Internet de las cosas médicas (IoMT) específicamente, que se refiere a un ecosistema ciberfísico de objetos de detección y activación interconectados dentro del sector de la salud (VerFigura 1) [3]. Estos dispositivos constituyen un riesgo importante para la seguridad debido a su ubicuidad y salvaguardias relativamente inmaduras [4,5]. A continuación, analizamos las posibles secuelas de los daños cibernéticos en la medicina, analizamos los esfuerzos regulatorios hasta la fecha y describimos las amenazas emergentes en la seguridad “inteligente” para la atención médica.

Taxonomía del daño

Cualquier dispositivo que utilice una red o un sistema de información corre el riesgo de ser pirateado. Los ciberataques caen en un continuo de descarado a imperceptible, lo que tiene implicaciones en términos de detección y respuesta. También vale la pena señalar que, si bien el término "ciberataque" a menudo se combina con intenciones maliciosas, las brechas de seguridad accidentales pueden amenazar igualmente la seguridad del paciente. Ilustramos los efectos del ciberataque por medio de un marco de seguridad canónico, extrayendo tanto del contrafáctico como del pasado.

tabla 1
Glosario de términos y abreviaturas clave.

Término	Definición
La seguridad cibernética	Medida para salvaguardar la confidencialidad, integridad y disponibilidad de tecnología y datos digitales.
Dispositivo médico	Elementos utilizados para la prevención, el diagnóstico, el tratamiento o la cura de enfermedades.
Internet de las Cosas (IoT)	Un ecosistema ciberfísico de objetos sensores y actuadores interconectados.
Sensor	Entidad que detecta indicadores físicos y los convierte en señal digital.
Solenoide	Entidad que manipula una salida física en respuesta a una señal digital.
Bluetooth	Tecnología inalámbrica que permite la comunicación del dispositivo mediante la transmisión de paquetes de datos a distancias cortas.
Usables	Dispositivos que interactúan externamente con el cuerpo humano, lo que les permite llevarlos y quitarlos fácilmente.
Implantables	Dispositivos con un componente (s) que interactúa internamente dentro del cuerpo humano.
Software malicioso	Software de código que se puede utilizar para dañar o deshabilitar dispositivos.
Negación de servicio (DoS)	Un ataque que sobrecarga el ancho de banda de IoT, la memoria y las limitaciones de la batería, generalmente al inundar la red con tráfico.
Botnet	Un ejército de dispositivos secuestrados para inundar una red en un ataque de denegación de servicio.
Bluetooth de baja energía (BLE)	Una variante de Bluetooth con menor consumo de energía que mantiene un rango operativo similar.
Listo para usar (OTS)	Componentes fabricados por proveedores externos que los fabricantes pueden utilizar para asociarlos o integrarlos en sus dispositivos para el control operativo, la funcionalidad o el suministro de energía.
Inteligencia artificial (AI)	La aplicación de algoritmos informáticos para realizar tareas generalmente asociadas a la inteligencia humana.
Computación en la nube	Uso de servidores en Internet para ejecutar software y bases de datos.
Computación de borde	Uso de servidores cercanos al dispositivo para el procesamiento de datos. Uso
Computación cuántica	de la mecánica cuántica para generar estados de procesamiento paralelo que operan simultáneamente para aumentar la potencia y la funcionalidad de la computación.
Criptografía	Protección de las comunicaciones mediante la conversión de datos dentro (cifrado) y saliendo (descifrado) de un formato seguro. Leger
Blockchain	digital para el almacenamiento descentralizado de datos que utiliza técnicas criptográficas.

ejemplos (ver Figura 2). Es de destacar que este esquema de clasificación no pretende ser exhaustivo, y los principios mecanicistas del ciberataque se ilustran a grandes rasgos, ya que están pensados como una descripción general para los responsables de la formulación de políticas y los profesionales de la salud.

Confidencialidad

La pérdida de confidencialidad se refiere tradicionalmente a divulgaciones no autorizadas de información del paciente protegida por el código legal federal. En el contexto de amenazas externas, esto suele ocurrir debido a un acceso no autorizado, robo de dispositivos o ataque de malware. Primero, un dispositivo pirateado podría usarse como conducto para espiar información de salud por parte de un actor no autorizado. La autenticación de acceso a la red y el cifrado de los datos del dispositivo de IoT pueden reducir este tipo de ataque, pero los incidentes pasados han demostrado que estas mejores prácticas no siempre están vigentes.[6–8]. Incluso si el Internet de las cosas médicas está debidamente protegido, la llegada de entornos inteligentes también plantea la posibilidad de que el Internet de las cosas adyacente a la salud sea un nuevo vector de ataque. Este principio no está mejor ilustrado que el infame atraco cibernético al casino de 2017 [9,10]. En este truco, los adversarios utilizaron una pecera inteligente en el vestíbulo para acceder a la red del casino y luego pudieron extraer varios gigabytes de información de la base de datos de grandes apostadores. El robo de IoT es otro método que se puede utilizar para extraer datos o credenciales del dispositivo y destaca la importancia de la seguridad física.[11]. Este riesgo se ve agravado por el hecho de que los dispositivos de IoT con frecuencia se pueden ocultar y a menudo se encuentran en áreas con acceso físico sin restricciones. Las mitigaciones para el robo pueden incluir equipar IoT portátil de alto riesgo con rastreadores de ubicación vinculados a alertas de actividad sospechosa.
[12]. Por último, los piratas informáticos también pueden infectar dispositivos con programas de malware para su uso en la vigilancia o extracción de datos.

Las amenazas internas pueden clasificarse como intencionales o inadvertidas y son el resultado de la creación de una "puerta trasera" que introduce una apertura para un ataque posterior. Los ataques de malware a menudo aprovechan este tipo de error interno. Tomemos un ataque de phishing, por ejemplo, que, una vez que un paciente o personal médico desprevenido hace clic en él, propaga software espía desde una computadora a dispositivos cercanos. La educación en torno a la concienciación sobre ciberataques es una forma de ayudar a reducir este tipo de ataque[13]. El mantenimiento y el mantenimiento oportunos del dispositivo también son vitales para una buena higiene de seguridad[14]. Estas prácticas incluirían cualquier cosa, desde la instalación oportuna de actualizaciones o parches hasta la atención al final de la vida útil del dispositivo. No purgar correctamente un dispositivo antes de desecharlo, por ejemplo, podría dejarlo vulnerable a la extracción de datos. Los dispositivos mal colocados también conllevarían un perfil de riesgo similar. Finalmente, un ejemplo muy común de falla interna es descuidar el cambio de las contraseñas predeterminadas en los dispositivos inteligentes, que los adversarios pueden aprovechar para obtener privilegios de acceso [15, dieciséis].

Integridad

La integridad es la confiabilidad de un dispositivo. En términos generales, la pérdida de la integridad del dispositivo puede deberse a la corrupción de la funcionalidad o los datos. Un ejemplo clásico es el armamento directo de un dispositivo médico mediante un ataque de reprogramación. Este tipo de piratería puede provocar una amplia gama de efectos según la aplicación clínica del dispositivo. Por ejemplo, la apropiación de dispositivos que se asocian íntimamente con el cuerpo, como implantables o bombas, podría provocar directamente la muerte o lesiones corporales. La manipulación cognitiva sutil, como la manipulación de dispositivos de neuroestimulación, podría ser más difícil de detectar. Ya en 2008, los investigadores demostraron que la piratería maliciosa de dispositivos médicos era técnicamente factible en el entorno de laboratorio.[17]. El grupo pudo ajustar el programador del dispositivo de un marcapasos para escuchar a escondidas, alterar los datos del paciente, interrumpir las comunicaciones, producir interferencias y manipular la administración de descargas.[17]. Este no es de ninguna manera un incidente aislado, y los ejemplos recientes también han afianzado el IoMT

[18]. Tomemos, por ejemplo, la vulnerabilidad de 2016 en el calcetín Owlet Smart, un monitor para bebés repleto de sensores que los padres pueden usar para rastrear la frecuencia cardíaca y la saturación de oxígeno de su bebé en su teléfono.[18]. Un investigador de seguridad descubrió que las comunicaciones de Smart Sock con Owlet

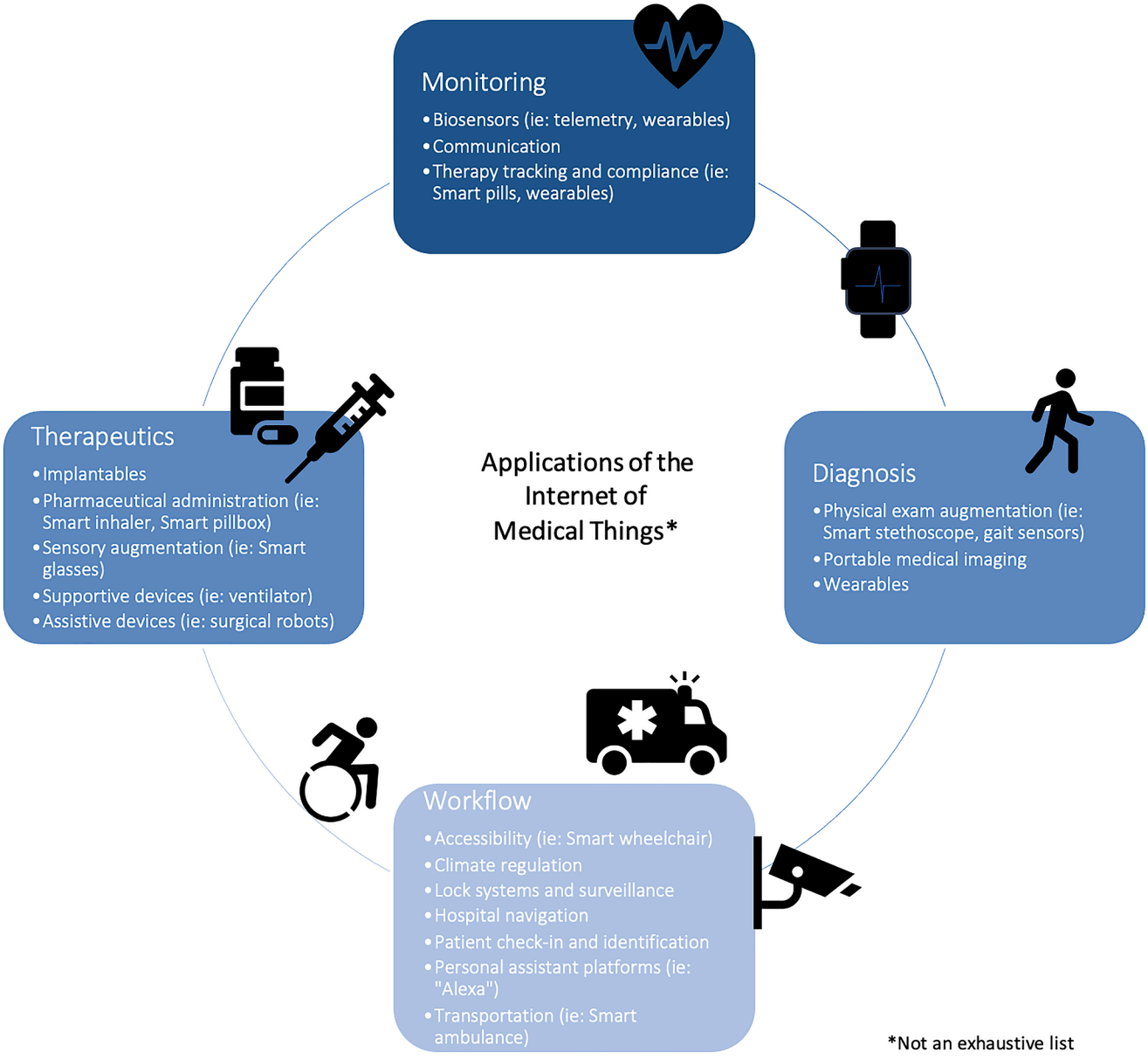

Figura 1. Aplicaciones de Internet de las cosas médicas.

la estación de enrutamiento de datos se mantuvo en una red no autenticada sin cifrado [18]. Un adversario podría haber aprovechado fácilmente la vulnerabilidad para silenciar, generar o interferir de otra manera con las alarmas del monitor para bebés de forma remota.

Los dispositivos también pueden verse comprometidos mediante el sabotaje de la integridad de los datos. Por ejemplo, un actor malintencionado podría inyectar entradas deliberadamente o instalar malware para dañar los datos del dispositivo. Por lo tanto, este tipo de ataque interrumpe cualquier proceso de dispositivo basado en datos. Las posibles secuelas de un ataque de este tipo pueden incluir una calibración inexacta del dispositivo, un diagnóstico erróneo o errores de tratamiento. [19]. Considere el escenario hipotético de un paciente con presión arterial alta e insuficiencia cardíaca crónica que usa un pastillero inteligente para administrar sus múltiples medicamentos. Se podría usar un ataque de inyección de datos en el pastillero para duplicar la dosis del medicamento diurético del paciente o para engañar al dispositivo haciéndole creer que el medicamento ya se había administrado. Esto podría inducir efectos nocivos sobre la presión arterial del paciente que podrían resultar en lesiones asociadas a la hipoperfusión o la muerte.

Disponibilidad

La disponibilidad se refiere a la capacidad de un dispositivo para ser utilizado por una parte autorizada. Esta propiedad está limitada por limitaciones de ancho de banda, memoria y batería. Los ataques de denegación de servicio (DoS) sobrecargan un dispositivo, generalmente inundando la red con tráfico. Un ataque DoS podría utilizarse para agotar la batería de un marcapasos, por ejemplo[20]. Alternativamente, al saturar la memoria de un reloj inteligente, se podría hacer que el dispositivo no responda o forzar un reinicio. Este último es solo una secuela demostrada de las vulnerabilidades "SweynTooth" de marzo de 2020 en el "sistema en un chip" de Bluetooth Low Energy (BLE)[21]. En términos generales, el consumo reducido de energía de BLE lo convierte en una opción atractiva y ampliamente utilizada para dispositivos con pocos recursos como IoT. Sin embargo, un grupo de investigadores de Singapur identificó una serie de fallas en la pila de protocolos de los principales componentes BLE listos para usar (OTS) que se utilizan para el emparejamiento de dispositivos.[21]. El alcance de SweynTooth fue enorme, implicando a más de 480 líneas de productos en múltiples sectores y destacando la necesidad de prestar atención a la seguridad en los artículos OTS.[21]. Las vulnerabilidades se pueden aprovechar principalmente mediante tácticas DoS con un ataque.

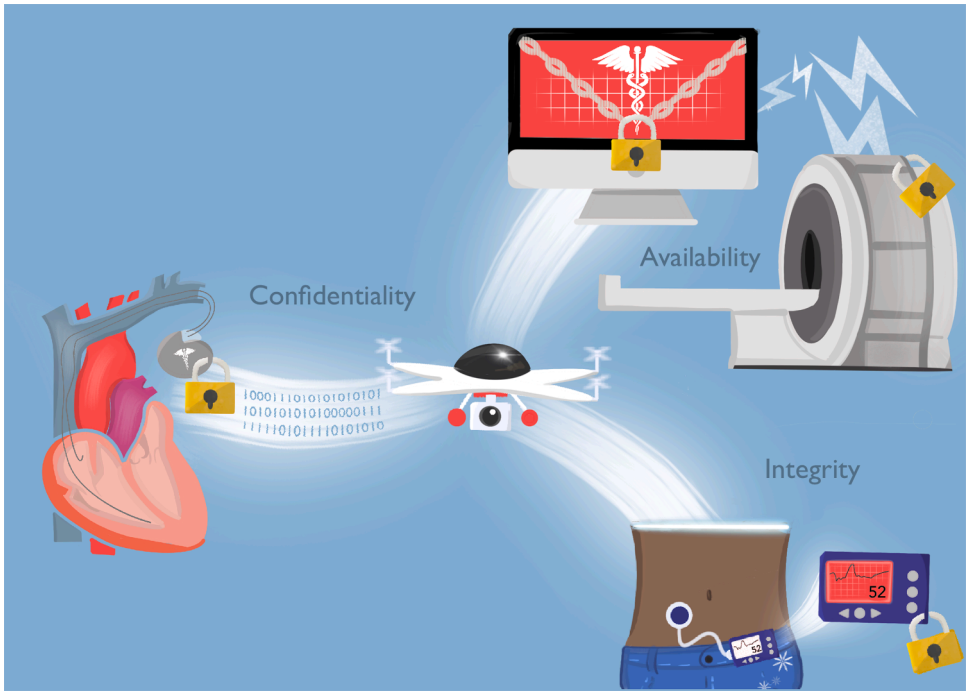

Figura 2. Vectores de ataque novedosos en un mundo de Internet de las cosas. La figura ilustra los tres principios de la tríada de seguridad de la CIA con un dispositivo IoT, en este caso un dron, como vector de ataque. (Izquierda) Se está extrayendo información de un marcapasos, lo que representa una violación de la confidencialidad. (Abajo a la derecha) La integridad está representada por una reprogramación no autorizada en una bomba de insulina. (Arriba a la derecha) Por último, el dron ejecuta un ataque DoS en una máquina de resonancia magnética, lo que hace que no se pueda usar.

radio restringido al alcance de Bluetooth [21]. Los dispositivos de IoT para el cuidado de la salud potencialmente afectados iban desde dispositivos portátiles como bandas de fitness y audífonos hasta terapias inteligentes como marcapasos e inhaladores.[21]. Es de destacar que, si bien la mayoría de los ataques DoS causan interrupciones temporales del servicio, como es el caso de SweynTooth, otros incidentes han demostrado que también es posible "bloquear" o deshabilitar permanentemente (PDoS) los dispositivos IoT [15,22].

Los ejemplos anteriores se pueden vincular a consecuencias directas para la seguridad del paciente, pero también se sabe que los ataques DoS causan interrupciones en el flujo de trabajo. Esto puede manifestarse como retrasos en la atención o daños económicos, que ejercen una presión sobre el sistema de salud [23,24]. De particular preocupación aquí es el potencial de un ataque distribuido de denegación de servicio (DDoS) a gran escala que explote Internet of Medical Things. Tomemos como ejemplo la campaña DDoS “Mirai” en la empresa de infraestructura de Internet Dyn en 2016. El ataque reclutó a numerosos IoT domésticos que usaban contraseñas predeterminadas en un ejército de "bots" que se usó para inundar la red Dyn [25,26]. El ataque cibernético resultó en interrupciones generalizadas del servicio en muchos sitios, incluidos Amazon, Netflix, Twitter y Spotify, entre otros.[26]. La parte responsable luego lanzó el código Mirai como código abierto en la web, generando una serie de iteraciones sucesivas que continúan avanzando en términos de alcance y complejidad.

Regulación de EE. UU.

La Administración de Alimentos y Medicamentos (FDA) es el guardián nacional de la ciberseguridad de los dispositivos médicos en los EE. UU. Ya en 2005 y para adelantarse al problema, la FDA abordó por primera vez el tema de la seguridad de los dispositivos médicos. Su "Ciberseguridad para dispositivos médicos en red que contienen software estándar" tomó la forma de una breve guía de preguntas y respuestas.[27]. Los documentos de orientación completos previos y posteriores a la comercialización para la industria seguirían más adelante en 2014 y 2016, respectivamente [28,29]. La guía previa a la comercialización aprovecha el "Marco para mejorar la ciberseguridad de la infraestructura crítica" del Instituto Nacional de Estándares y Tecnología (NIST) para promover un enfoque de "seguridad por diseño" para la fabricación de dispositivos.[30]. El enfoque deliberadamente amplio del marco prioriza los principios generales de seguridad sobre el cumplimiento de requisitos rígidos para fomentar la flexibilidad y la innovación.[30]. En septiembre de 2017 y en

En respuesta a una tendencia de toda la industria hacia arquitecturas de dispositivos más complejas, la FDA emitió las “Consideraciones de diseño y recomendaciones de presentación previa a la comercialización de dispositivos médicos interoperables”. Se pidió a los fabricantes que documentaran el propósito previsto para las comunicaciones del dispositivo, los usuarios anticipados adicionales, los controles de autenticación y los dispositivos de socios aprobados.[31]. Finalmente, en un esfuerzo por promover la transparencia, la FDA publica comunicaciones públicas sobre las vulnerabilidades cibernéticas de los dispositivos que, si se actúa, podrían resultar en daños al paciente (ver Tabla 2) [32]. La FDA aún no ha recibido informes de daños a pacientes asociados con vulnerabilidades cibernéticas en dispositivos médicos [32,33].

Otras iniciativas históricas con un enfoque en la seguridad inteligente incluyen el "Informe interinstitucional sobre el estado de la estandarización internacional de ciberseguridad para IoT" del NIST, que se publicó en noviembre de 2018. Este documento mapea los riesgos en el panorama de amenazas de IoT a documentos de orientación de seguridad relevantes en todos los sectores. , con el sector de la salud recibiendo las más altas calificaciones en la disponibilidad de estándares básicos de ciberseguridad en seguridad física y de redes [34]. Los elementos clave en la agenda exploratoria son blockchain para criptografía, manejo de incidentes que no son susceptibles de parcheo, administración de conectividad de red espontánea y automatización de seguridad.[34]. La "Base de referencia básica de la capacidad de ciberseguridad de dispositivos de IoT" fue lanzada posteriormente por el NIST en junio de 2019 como una guía agnóstica y fácilmente digerible para los fabricantes que consolida las propiedades para asegurar mínimamente los dispositivos de IoT. Estos principios básicos incluyen identificación de dispositivos, configuración autorizada, protección de datos, acceso restringido, actualizaciones de software y detección (verFig. 3) [35]. Las direcciones de supervisión futuras en el ámbito cibernético en general tienen como objetivo reforzar la autoridad federal en torno a IoT[36]. De hecho, la reciente Ley de Mejora de la Ciberseguridad de IoT se convirtió en ley el 4 de diciembre de 2020 y requerirá que todos los dispositivos comprados por el gobierno cumplan con los estándares mínimos de ciberseguridad que definirá el NIST, lo que aumenta la posibilidad de modificaciones adicionales a las medidas existentes de la FDA.[36].

Cabe señalar que, si bien los documentos de orientación federales antes mencionados sirven como excelentes marcos conceptuales, no se asignan explícitamente a los procesos de diseño de fabricación existentes. Para reflejar mejor las prácticas estándar de la industria, el sector privado también ha desarrollado una serie de estándares de consenso que ofrecen un lenguaje y

Tabla 2

Comunicaciones de seguridad de ciberseguridad de la Administración de Drogas y Alimentos de EE. UU. Hasta la fecha

* Tenga en cuenta los cambios en el alcance y el tipo de dispositivo a lo largo de los años.

Año	Fabricante	Tipo de dispositivo (s)	Alcance	Vulnerabilidades
2015	Hospira	Droga hospitalaria bomba de infusión	-	Remoto no autorizado el usuario podría remotamente manipular drogas Dosis
2017-18	Abbott (Anteriormente St. Jude Medical)	Implantable marcapasos	465.000 implantado dispositivos en los Estados Unidos	Remoto no autorizado el usuario podría reprogramar el dispositivo para provocar el agotamiento de la batería o no autorizado estimulación / descargas
2018	Medtronic	Implantable marcapasos	-	Remoto no autorizado el usuario podría atacar durante el software actualizaciones si se usa Internet conexión con el software distribución la red
2019	Medtronic	Implantable marcapasos y desfibrilador	-	No autorizado el usuario podría alterar configuración de dispositivo cuando la telemetria en uso cuando muy cerca distancia
		Bomba de insulina	400.000 bombas en usar	No autorizado el usuario podría de forma inalámbrica manipular administración de insulina cuando dentro quemarropa
2019	Múltiple, Sector de salud "Urgente / 11"	Dispositivos conteniendo operando sistemas con Software de IPnet componente	200 millones + dispositivos y IoT	Remoto no autorizado usuario, DoS o fuga de información ataques
2020	GE Healthcare	Telemetría dispositivo para hospital seguimiento de paciente vital señales	- -	Remoto no autorizado el usuario podría remotamente silencio, generar, o de lo contrario interfiere con alarmas
2020	Múltiple, Todo Sectores "SweynTooth"	Dispositivos con BLE afectado sistema en un chip vendido por siete industrias vendedores	480+ producto líneas	No autorizado usuario, DoS o fuga de información ataca cuando dentro de la BLE distancia

alineación. Los documentos más influyentes en este campo son posiblemente las series TIR57 y UL 2900 de la Asociación para el Avance de la Instrumentación Médica (AAMI), ambas aprobadas formalmente por la FDA. Una de las fortalezas de la serie AAMI TIR57 radica en su enfoque integral para la gestión de riesgos en lo que respecta a la identificación de amenazas específicas del dispositivo y su evaluación preventiva, controles de diseño y monitoreo longitudinal.[37]. La serie UL 2900 contiene consideraciones previas y posteriores a la comercialización, pero es ampliamente reconocida por la solidez de sus estrategias de prueba y mitigación que aprovechan el Common Vulnerability Scoring System (CVSS) para una indexación uniforme de la gravedad del incidente.[38].

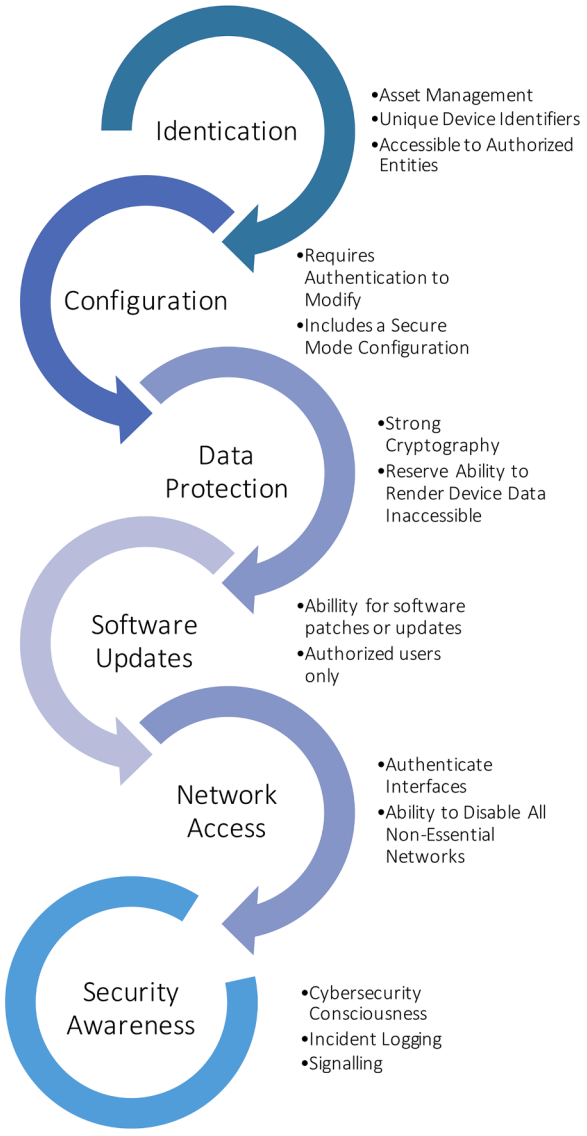

Fig. 3. Principios básicos básicos de la capacidad de ciberseguridad de dispositivos de IoT del Instituto Nacional de Estándares y Tecnología de EE. UU.

Gobernanza internacional

El Foro Internacional de Reguladores de Dispositivos Médicos (IMDRF) es un colectivo de líderes mundiales del sector público y privado que trabajan para desarrollar estándares de consenso mundial. El nuevo Grupo de Trabajo sobre Ciberseguridad de la IMDRF, copresidido por Canadá y EE. UU., Se reunió por primera vez en el otoño de 2019. Los esfuerzos iniciales culminaron en el documento de orientación “Principios y prácticas para la ciberseguridad de los dispositivos médicos” de la IMDRF. Con respecto a las consideraciones previas a la comercialización, el IMDRF subraya la importancia de las evaluaciones integrales de riesgos y destaca las matrices de trazabilidad que vinculan cada amenaza con sus respectivos controles de ciberseguridad como un enfoque estándar de oro.[11]. Otro control clave previo a la comercialización señalado por la IMDRF son las pruebas de seguridad sólidas. Estas evaluaciones deben tener en cuenta cualquier vulnerabilidad conocida en cualquiera de los componentes del dispositivo a través de enfoques específicos y también intentar identificar posibles vulnerabilidades desconocidas en el dispositivo o su ecosistema, como a través de pruebas de penetración y análisis de variantes.[11]. Entre los artículos de posventa, hay un claro énfasis en la transparencia internacional y la indexación uniforme de los incidentes cibernéticos.[11]. Aquí, el CVSS y la "Guía del equipo de respuesta ante emergencias informáticas para la divulgación coordinada de vulnerabilidades" se indican como ejemplos de referencia.[11]. El grupo tiene

Aún no hemos profundizado en las consideraciones para el IoT médico específicamente, sino que presenta principios generales para la seguridad y la coordinación de los dispositivos en general. [11].

Amenazas emergentes

Inteligencia artificial

La heterogeneidad en los dispositivos de IoT conduce a una amplia variedad de enfoques de eliminación. Un ser humano no tiene por qué estar siempre en el lado del adversario. Los algoritmos, bots y drones cada vez más sofisticados ya pueden utilizarse como vectores de ataque (verFigura 2) [39–41]. Los piratas informáticos también pueden aprovechar estas tecnologías para mejorar las capacidades de ataque en términos de eficiencia, accesibilidad y escalabilidad. La utilización de armas cibernéticas de la inteligencia artificial podría muy bien convertirse en una nueva norma. Por otro lado, estas características también tienen compensaciones de seguridad [41,42]. El código adaptable se basa en gran medida en los datos entrantes. Por lo tanto, un ataque adverso sutil a los datos de entrada tiene el potencial de alterar los algoritmos en silencio, dejando apenas un rastro. Además, la pérdida de la arquitectura estática relega el concepto tradicional de "depuración" a una cosa del pasado.[41]. Otra consideración de seguridad rodea la perspectiva de los algoritmos de inteligencia artificial como sistemas ciberfísicos que actúan de forma autónoma.[43]. Un ejemplo clásico de esto serían los dispositivos arrastrados por retroalimentación visuoespacial en tiempo real, es decir, un robot quirúrgico. Este tipo de tecnología puede ser vulnerable a la manipulación física sutil del campo visual del dispositivo, por ejemplo, mediante láseres brillantes, que puede provocar errores de clasificación o de toma de decisiones [44,45]. Si bien los humanos generalmente pueden detectar este tipo de errores, puede ser difícil detectarlos en dispositivos médicos fuera del circuito [41,43]. El monitoreo automatizado de eventos con IA de defensa puede proporcionar una solución para la detección y posible contrarrestar estas infracciones [46,47].

Convergencia de la nube

A continuación, vemos que los datos como una mercancía son un objetivo en movimiento. [2]. Si bien los ataques cibernéticos a la información médica protegida en el dispositivo siguen siendo un problema importante, los piratas informáticos están diversificando sus carteras. La investigación médica, los acuerdos contractuales, los datos de pacientes no relacionados con la salud y la información empresarial se encuentran ahora cada vez más entre los objetivos cibernéticos.[48]. El punto a destacar aquí es que el cumplimiento de las medidas de privacidad sobre los datos de salud por sí solo no se puede combinar con las salvaguardias de ciberseguridad adecuadas. Además, a medida que las plataformas informáticas consolidadas como la nube gestionan más dispositivos para construir un mundo más inteligente, es probable que este problema se agrave. Es necesaria la armonización de la seguridad de los dispositivos y la nube para garantizar la protección continua de los datos. Por ejemplo, si bien los requisitos de seguridad menos sólidos para IoT pueden ser aceptables en ciertos entornos de bajo riesgo, pueden crear una puerta trasera para los piratas informáticos si comparten bienes raíces con dispositivos médicos en la nube. Evaluar, restringir y podar las arquitecturas de la nube para que interactúen solo con interfaces confiables puede mitigar algunos de estos riesgos. Del mismo modo, los datos deben cifrarse siempre que sea posible con auditorías periódicas para garantizar el no repudio.

Otro espacio que merece atención es el área entre el dispositivo y la nube, conocida como el borde. La computación perimetral se refiere a micro centros de datos donde los datos del dispositivo se procesan localmente, a menudo antes de ser enrutados a la nube. Esta práctica está ganando terreno en la esfera de IoT por su capacidad para reducir la latencia del dispositivo y la transmisión de datos superfluos. [49]. En términos de implicaciones de seguridad, la computación en el borde puede ser beneficiosa al reducir la cantidad total de datos en tránsito y al distribuir el riesgo entre varios nodos distribuidos, en lugar de centralizarlos en la nube. Al mismo tiempo, esto también tiene el efecto adverso de aumentar la superficie total de ataque. Evitar la conectividad persistente de nodo a red al permitir una configuración segura para su uso durante los tiempos de inactividad de la computadora puede reforzar la seguridad. Por lo general, las comunicaciones directas de borde a nube también deben evitarse o requerir autenticación para las operaciones necesarias. Finalmente, las redes dedicadas y seguras deben usarse para la computación de borde en los sistemas de IoT de misión crítica en lugar de más

Redes públicas o privadas virtuales vulnerables.

Reequipamiento

Los avances recientes en IoT añaden otro aspecto de complejidad a la práctica actual del apilamiento de dispositivos. El upcycling con IoT es una opción atractiva para proveedores y usuarios finales porque puede permitir una funcionalidad mejorada del dispositivo que, de otro modo, podría tener un costo prohibitivo. Sin embargo, la debilidad de la seguridad en el IoT más nuevo, bastante concebible dadas las tendencias hacia el IoT básico con baja potencia informática que se puede lanzar rápidamente al mercado, puede introducir un conducto para el ataque. Por el contrario, la simple adaptación de IoT a los entornos existentes puede propagar las fallas de la tecnología obsoleta a los dispositivos más nuevos. Este tipo de error de seguridad se ejemplificó en las recientes vulnerabilidades "Urgente / 11" en un sistema operativo antiguo que se trasladó e incrustó en cientos de millones de dispositivos médicos fabricados en EE. UU.[50]. Esta falla podría haberse aprovechado para permitir la eliminación masiva de dispositivos que ejecutaban este sistema operativo común, que iba desde bombas de infusiones hasta monitores de telemetría de pacientes. Es probable que los incidentes de ciberseguridad a gran escala como "Urgente / 11" ocurran con mayor frecuencia debido a las tendencias hacia una mayor interconectividad de IoT, el uso de artículos comunes disponibles en el mercado y la utilización prolongada de tecnologías "heredadas" obsoletas (ver Tabla 2). El cumplimiento obligatorio de la vida útil de los dispositivos admitidos, la implementación de requisitos de seguridad previos a la adquisición para los proveedores y la realización de evaluaciones de peligros integradas e individuales para los componentes del dispositivo también pueden ayudar a mitigar las malas prácticas de adaptación. Finalmente,

Computación cuántica

La computación cuántica capaz de producir una amenaza real a la seguridad podría llegar tan pronto como en las próximas una o dos décadas [51,52]. Una plataforma operativa de esta clase puede presumir de potencia y funcionalidad mejoradas al aprovechar la mecánica cuántica para procesar datos en estados paralelos. El desarrollo cuántico es relevante para nuestro análisis de la seguridad en el IoMT, ya que estas tecnologías tienen el potencial de hacer que muchos criptosistemas existentes y sus respectivas salvaguardas de seguridad queden obsoletos (es decir, cifrado de clave pública, blockchain, etc.). Un dilema anticipado radica en el hecho de que muchos códigos de cifrado se basan en la premisa de que el ancho de banda computacional necesario para descifrar el cifrado será demasiado oneroso para el funcionamiento de la computadora convencional. Las computadoras cuánticas podrían abrumar estos cálculos reforzados con sus mayores capacidades de procesamiento. Si bien muchos algoritmos de cifrado convencionales se verían comprometidos irremediablemente, otros podrían hacerse resistentes a los cuánticos. Esta criptografía "post-cuántica" es un área de investigación emergente con posibles mitigaciones que incluyen la modificación del tamaño y los parámetros de la clave o mediante el uso de cifrados redundantes.[53]. A corto plazo, los fabricantes deberían realizar evaluaciones de peligros en torno a la resiliencia cuántica de sus tecnologías para gestionar sus activos de poscomercialización y orientar sus prioridades de desarrollo posteriores. A largo plazo, puede estar indicado un cambio de paradigma completo hacia la criptografía cuántica segura para garantizar la seguridad sanitaria continua.[53]. Dado que los expertos encuentran que la "eliminación gradual de un algoritmo de cifrado en peligro puede llevar una década o más", la planificación de la transición para las tecnologías de misión crítica de IoMT debería comenzar ahora.[53]. Por otro lado, una solución definitiva para la defensa cuántica puede incorporarse al problema en sí. De hecho, la perspectiva del cifrado cuántico también se vislumbra en el horizonte, que podría producir un cifrado teóricamente imposible de descifrar aprovechando las propiedades de entrelazamiento de la mecánica cuántica.

Empoderando a los usuarios finales

Una de las formas más impactantes para que los usuarios finales y el personal sanitario aliado ayuden con la defensa cibernética es a través de la activación oportuna de la cascada de informes de eventos. La identificación rápida de posibles infracciones cibernéticas es esencial para minimizar el daño al paciente, agilizar la mitigación de amenazas y prevenir la propagación viral a otros dispositivos. Los canales de información de eventos de la institución y los protocolos de respuesta ad hoc para los proveedores médicos deben introducirse durante el proceso de incorporación y revisarse periódicamente. Dichas entidades pueden incluir el departamento de TI, el personal de fabricación relevante y el equipo de gestión de incidentes hospitalarios, que posteriormente pueden activar los canales ascendentes adecuados.[54]. Los médicos independientes y los pacientes a menudo también tienen una línea directa con la supervisión central a través del canal de informes MedWatch de la FDA de EE. UU., Que se puede utilizar para rastrear las tendencias a nivel nacional en el comportamiento aberrante de los dispositivos médicos.[55]. El personal sanitario, los oficiales de mando de incidentes, los enlaces de la industria, el personal de respuesta a emergencias y otras partes interesadas relevantes también deben participar en las capacitaciones destinadas a promover la concienciación y la preparación ante ciberataques [56]. Dichos simulacros deben considerar activaciones en el campo, pacientes hospitalizados y ambulatorios y deben adaptarse al inventario de IoT de la institución y a la población de pacientes local. Los ejemplos pueden incluir un incidente de víctimas masivas como resultado de un ataque diseminado contra IoMT en la comunidad o un robot quirúrgico secuestrado, por nombrar algunos.

Los profesionales de la salud y el personal aliado también deben esforzarse por fomentar un espíritu de seguridad en torno a la ciberseguridad de los dispositivos médicos en sus encuentros de rutina con los pacientes. Los proveedores médicos o técnicos que están manejando dispositivos con pacientes deben reservar tiempo durante la visita inicial o previa a la implantación para establecer un plan de seguridad cibernética en caso de que el dispositivo no funcione correctamente. Garantizar el cumplimiento del paciente con los sistemas operativos recomendados y las actualizaciones o parches de ciberseguridad es igualmente vital. Dado que no se puede asumir la alfabetización en salud y tecnología entre los pacientes, los trabajadores de la salud y el personal afiliado servirán como traductores de conocimientos críticos para los pacientes cuando surjan vulnerabilidades de ciberseguridad. De esta manera, es importante que los proveedores mantengan un conocimiento práctico de los próximos pasos para las mitigaciones técnicas, posibles implicaciones para la salud y protocolos de emergencia en caso de una ciber emergencia. El desarrollo de materiales educativos en torno a la promoción de la seguridad personal de IoT a nivel local o federal también puede servir como una estrategia de mitigación preventiva, como se hace habitualmente para otras crisis de salud pública como la adicción a las drogas, la violencia armada o COVID-19. Estos materiales pueden incluir buenas prácticas de higiene de seguridad personal, como la protección de los identificadores de dispositivos y la información de contraseñas, el cambio de contraseñas predeterminadas, la desactivación de Bluetooth cuando no se usa IoT y la auditoría de IoT en redes personales, por nombrar algunos (consulte como se hace habitualmente para otras crisis de salud pública como la adicción a las drogas, la violencia armada o COVID-19. Estos materiales pueden incluir buenas prácticas de higiene de seguridad personal, como la protección de los identificadores de dispositivos y la información de contraseñas, el cambio de contraseñas predeterminadas, la desactivación de Bluetooth cuando no se usa IoT y la auditoría de IoT en redes personales, por nombrar algunos (consulte como se hace habitualmente para otras crisis de salud pública como la adicción a las drogas, la violencia armada o COVID-19. Estos materiales pueden incluir buenas prácticas de higiene de seguridad personal, como la protección de los identificadores de dispositivos y la información de contraseñas, el cambio de contraseñas predeterminadas, la desactivación de Bluetooth cuando no se usa IoT y la auditoría de IoT en redes personales, por nombrar algunos (consulteTabla 3). De hecho, pedimos una adaptación y síntesis de la literatura sobre sistemas de salud y ciberseguridad para abordar las preocupaciones emergentes en las tecnologías de IoMT cada vez más ubicuas.

Conclusión

Los dispositivos inteligentes que aprovechan las redes pueden lograr un control mejorado sobre la fisiología humana, dando un significado completamente nuevo al término medicina de precisión. La salud digital nos acerca a nuestro objetivo de desarrollar un sistema de atención médica de aprendizaje, pero también deja a los pacientes cada vez más susceptibles a las vulnerabilidades en sus contrapartes de dispositivos. Esta precaria alineación de motivación, medios y oportunidades crea una tormenta perfecta para la piratería del IoMT. En este nuevo clima, la medicina haría bien en mantener el ciberataque en su radar. Reconociendo este peligro claro y presente, varios actores públicos y privados están involucrados en la ciberregulación con la intención de promover la seguridad sin sofocar la innovación. Avanzando

Tabla 3
Panorama de amenazas de Internet de las cosas médicas.

Amenaza	Mecanismo probable	Mitigaciones primarias
IA autónoma	Un sistema de circuito cerrado sería particularmente vulnerable a los ataques que envenenan los datos o distorsionan el espacio de trabajo visoespacial, los cuales pueden modificar las salidas del dispositivo.	Sistemas: Realice análisis preventivos de riesgos y costos / beneficios antes de la implementación para determinar la idoneidad y las posibles indicaciones de supervisión. Llevar a cabo auditoría automatizada, detección de intrusiones y contrarrestar con inteligencia artificial de defensa. Equipe IoT con apagado de emergencia y anulación manual capacidades. Usuario final: realizar una emergencia simulaciones para escenarios de alto riesgo (por ejemplo: robots quirúrgicos, ventilador).
Bluetooth/ Bluetooth bajo Energía	Lo más probable es que un ataque se dirija a la implementación de la pila de protocolos utilizada en el emparejamiento de dispositivos.	Sistemas: Implementar controles de autenticación para limitar los espontáneos Conectividad Utilice criptografía sólida para proteger comunicaciones. Usuario final: los usuarios deben apagar Bluetooth cuando no está en uso para evitar espontáneo Conectividad Mantenga actualizado el software de IoT relevante. Sistemas: mantenga actualizaciones de seguridad en la nube, autentique las comunicaciones, audite regularmente los activos, use redes aisladas para operaciones de misión crítica, implemente detección de intrusiones y cifrado de datos y copias de seguridad. Usuario final: proteja las contraseñas de la cuenta.
Nube Convergencia	Un ataque que explota la seguridad débil en IoT como conducto para atacar la nube.	
Computación de borde	El procesamiento distribuido puede aumentar la superficie potencial de ataque, con la interfaz de borde a nube particularmente en riesgo.	Sistemas: evitar la conectividad persistente de nodo a red. Inicie comunicaciones directas de borde a nube solo cuando sea absolutamente necesario con autenticación. Utilice redes seguras y dedicadas para los sistemas de IoMT de misión crítica.
Heterogeneidad de IoT y ubicuidad	La creciente diversidad de IoT introduce la posibilidad de nuevos atacantes y presas.	Sistemas: extrapole una amplia gama de escenarios durante el modelado de amenazas. Implementar contratos de usuario para que IoT se conecte a redes en redes de alto riesgo (es decir: Smart Hospital) que pueden facilitar la identificación, la gestión de activos y el seguimiento. Usuario final: Survey IoT conectado a personal redes para cualquier dispositivos no autorizados.
Fuera de la plataforma (OTS) Componentes	La utilización generalizada de componentes OTS en IoT crea un objetivo óptimo para los atacantes.	Sistemas: implementar requisitos de seguridad de OTS previos a la adquisición para los proveedores. Realizar integradas y seguridad individual evaluaciones de componentes.
Físico Medio ambiente	Un atacante puede explotar el dispositivo a través del acceso directo a IoT en áreas públicas mediante el robo de IoT ocultable.	Sistemas: equipe todo IoT con identificadores únicos y seguimiento / vigilancia para aquellos que son de alto riesgo. Tenga en cuenta todos los activos de IoT, en particular aquellos en redes de acceso público que comparten redes con activos de la institución (es decir, atraco a una pecera). Aislar los sistemas de misión crítica en

(*Continúa en la siguiente página*)

Tabla 3 (*continuado*)

Amenaza	Mecanismo probable	Mitigaciones primarias
		redes seguras. Usuario final: habilite el seguimiento en los dispositivos cuando corresponda e informe los dispositivos perdidos o robados.
Reequipamiento	La vulnerabilidad en un dispositivo obsoleto sirve como punto de compromiso de la red de IoT más grande.	Sistemas: las autoridades federales pueden exigir el cumplimiento de la vida útil de los dispositivos admitidos, regular el costo de las tecnologías médicas para aliviar el bloqueo financiero. Las instituciones pueden realizar análisis de peligros en tecnologías heredadas y podar arquitecturas de sistemas respectivamente. Usuario final: Examine el IoT conectado a redes personales para obtener actualizaciones y considere la posibilidad de eliminar los dispositivos que ya no admiten actualizaciones (es decir, cámaras web y enrutadores antiguos).
Cuántico Informática	Capacidades informáticas dejaría obsoletos muchos criptosistemas existentes.	Sistemas: los algoritmos de cifrado viables a menudo se pueden hacer resistentes a los aumentar el tamaño de la clave o los parámetros. Considerar la transición de la tecnología de misión crítica existente a cifrado cuántico seguro a corto plazo. Explore el desarrollo de la cuántica el cifrado como posible solución definitiva.

Aprobación ética

No requerido

Financiamiento / apoyo

Ninguno.

Conflicto de intereses

La Sra. Thomasian declara no tener ningún conflicto de intereses. El profesor Adashi se desempeña como copresidente del Consejo Asesor de Seguridad de Ohana Biosciences, Inc.

Referencias

[1] La FDA informa a los pacientes. Proveedores y fabricantes sobre posibles vulnerabilidades de seguridad cibernética para dispositivos médicos conectados y redes de atención médica que utilizan cierto software de comunicación [comunicado de prensa]. MD: Silver Spring; 1 de octubre de 2019.

[2] Cohen IG, Hoffman S, Adashi EY. ¿Su dinero o la vida de su paciente? Ransomware y registros médicos electrónicos. Ann Intern Med 2017; 167 (8): 587–8.

[3] Agencia de la Unión Europea para la Ciberseguridad (ENISA). Recomendaciones de seguridad de referencia para iot. enisaHeraklion, Grecia; 2017.

[4] Alsubaei F, Abuhussein A, Shiva S. Seguridad y privacidad en el Internet de las cosas médicas: taxonomía y evaluación de riesgos. En: 2017 IEEE 42nd Conference on Local Computer Networks Workshops (LCN Workshops). IEEE; 2017.

[5] Dimitrov DV. Internet médico de las cosas y big data en la asistencia sanitaria. Healthc Inform Res 2016; 22 (3): 156–63.

[6] Ching K, Mahinderjit Singh M. Análisis de vulnerabilidad de seguridad y privacidad de dispositivos de tecnología portátil. Int J Netw Sec Appl 2016; 8: 19–30.

[7] Radcliffe J. Hackear dispositivos médicos por diversión e insulina: rompiendo el sistema SCADA humano. En: diapositivas de presentación de la Conferencia Black Hat; 2011.

[8] Mohzary M, Tadisetty S, Ghazinour K. Una capa de protección de la privacidad para dispositivos portátiles. En: Simposio Internacional sobre Fundamentos y Práctica de la Seguridad. Saltador; 2019.

[9] Pelton JN, Singh IB. Retos y oportunidades en la evolución de internet de todo. Ciudades inteligentes de hoy y de mañana. Saltador; 2019. p. 159–69.

[10] Stremlau T. La motivación financiera para mantener segura la información. Comput Fraud Sec 2020; 2020 (2): 18–9.

[11] Grupo de trabajo de ciberseguridad de dispositivos médicos. principios y prácticas para la ciberseguridad de los dispositivos médicos. Foro internacional de reguladores de dispositivos médicos; 1 de octubre de 2019.

[12] Qusa H, Allam H, Younus F, Ali M, Ahmad S. Proteja el hogar inteligente con sistemas de inteligencia de seguridad abiertos. En: 2019 Sixth HCT Information Technology Trends (ITT). IEEE; 2019.

[13] Martin G, Martin P, Hankin C, Darzi A, Kinross J. Ciberseguridad y atención médica: ¿qué tan seguros estamos? BMJ 2017; 358: j3179.

[14] Ghafur S, Kristensen S, Honeyford K, Martin G, Darzi A, Aylin P. Un análisis de impacto retrospectivo del ciberataque de WannaCry en el NHS. NPJ Dig Med 2019; 2 (1): 98.

[15] Kolias C, Kambourakis G, Stavrou A, Voas J. DDoS en IoT: mirai y otras botnets. Computadora (Long Beach Calif) 2017; 50 (7): 80–4.

[dieciséis] MacDermott Á, Kendrick P, Idowu I, Ashall M, Shi Q. Asegurar las cosas en el Internet de las cosas de la atención médica. En: 2019 Global IoT Summit (GIoTS). IEEE; 2019.

[17] Halperin D, Heydt-Benjamin TS, Ransford B, Clark SS, Defend B, Morgan W, et al. Marcapasos y desfibriladores cardíacos implantables: ataques de radio por software y defensas zeropower. En: Simposio IEEE 2008 sobre seguridad y privacidad. IEEE; 2008.

[18] Thomson I. El monitor cardíaco para bebés con Wi-Fi puede tener la peor seguridad de IoT de 2016; 13 de octubre de 2016 [Disponible en:https://www.theregister.com/2016/10/13/p ossbly_worst_iot_security_failure_yet /? mt = 1476453928163.

[19] Maggi F, Quarta D, Pogliani M, Polino M, Zanchettin AM, Zanero S. Rogue robots: probando los límites de la seguridad de un robot industrial. tendencia micro. Politecnico di Milano; 2017. Representante técnico.

[20] Hei X, Du X, Wu J, Hu F. Defender los ataques de agotamiento de recursos en dispositivos médicos implantables. En: 2010 IEEE Global Telecommunications Conference GLOBECOM. 2010. IEEE; 2010.

[21] Matheus E. Garbelini SC, Chundong Wang. SweynTooth: Desatando el caos a través de Bluetooth de baja energía: Universidad de Tecnología y Diseño de Singapur; [Disponible de:https://asset-group.github.io/disclosures/sweyntooth/sweynt ooth.pdf.

[22] Equipo de respuesta a emergencias informáticas de los Estados Unidos (US-CERT). Ataque de denegación de servicio permanente BrickerBot; 12 de abril de 2017 [Disponible en: https://uscert.cisa.gov/ics/alerts/ICS-ALERT-17-102-01A.

[23] Martin G, Ghafur S, Kinross J, Hankin C, Darzi A. WannaCry: un año después. BMJ 2018; 361: k2381.

[24] Tully J, Selzer J, Phillips JP, O'Connor P, Dameff C. Desafíos de la salud en la era de la ciberseguridad. Sec de salud. 2020; 18 (3): 228–31.

[25] Newman LH Lo que sabemos sobre el apagón masivo de Internet en la costa este del viernes: cableado; 21 de octubre de 2016 [Disponible en: https://www.wired.com/2016/10/internet-outage-ddos-dns-dyn /.

[26] D. FitzGerald y R. McMillan. El ciberataque elimina el acceso a sitios web: Wall Street Journal; 24 de octubre de 2016 [Disponible en: https://www.wsj.com/articles/ denegación-de-servicio-ataque-web-afecta-amazon-twitter-otros-1477056080.

[27] Administración de Drogas y Alimentos de EE. UU. Ciberseguridad para dispositivos médicos en red que contienen software estándar (OTS). MD: Silver Spring; 2005.

[28] Administración de Drogas y Alimentos de EE. UU. Contenido de presentaciones previas a la comercialización para la gestión de la ciberseguridad en dispositivos médicos. Orientación para la industria y la alimentación y las drogas. Personal de administración; 2014.

[29] Administración de Drogas y Alimentos de EE. UU. Gestión postcomercialización de la ciberseguridad en dispositivos médicos. Orientación para el personal de la Industria y la Administración de Alimentos y Medicamentos; 2016.

[30] Instituto Nacional de Estándares y Tecnología. Marco para mejorar la infraestructura crítica. Ciberseguridad 2014.

[31] Administración de Drogas y Alimentos de EE. UU. Consideraciones de diseño y recomendaciones de presentación previa a la comercialización para dispositivos médicos interoperables. MD: Orientación para el personal de la Industria y la Administración de Alimentos y Medicamentos Silver Spring; 2017.

[32] Administración de Drogas y Alimentos de los Estados Unidos. Ciberseguridad [Disponible en:https: //www.fda.gov / dispositivos-médicos / salud-digital / ciberseguridad].

[33] Administración de Drogas y Alimentos de EE. UU. La FDA informa a los proveedores de atención médica. instalaciones y pacientes sobre posibles vulnerabilidades de seguridad cibernética para ciertas estaciones centrales de información clínica y servidores de telemetría de GE Healthcare; 23 de enero de 2020 [Disponible desde,https://www.fda.gov/news-events/press-announcements/fda-in forms-health-care-Suppliers-Facilities-and-Patients-about-potencial-cybersecurity.

[34] Grupo de Trabajo Interagencial Internacional de Normalización de la Ciberseguridad. Informe interinstitucional sobre el estado de la estandarización internacional de ciberseguridad para Internet de las cosas (IoT). Instituto Nacional de Estándares y Tecnología; 2018.

[35] Fagan M, Megas KN, Scarfone K, Smith M. Base de referencia básica de capacidad de ciberseguridad de dispositivos de IoT. Nat Inst Stand Technol 2020: S. 734.

[36] TIR57 A. Principios para la seguridad de los dispositivos médicos: gestión de riesgos. Arlington, VA: Asociación para el Avance de la Instrumentación Médica; 2016.

[37] UL. UL 2900. Norma de ciberseguridad de software para productos conectables a la red; 01 de septiembre de 2017.

[38] Greenberg A. Mira cómo un dron se apodera de una televisión inteligente cercana. Cableado; 11 de agosto de 2019 [Disponible en: https://www.wired.com/story/smart-tv-drone-hack/].

[39] Nassi B, Shamir A, Elovici Y. Xerox Day Vulnerability. IEEE Trans Inf Forensics Sec 2018; 14 (2): 415–30.

[40] Brundage M, Avin S, Clark J, Toner H, Eckersley P, Garfinkel B, et al. El uso malintencionado de la inteligencia artificial: previsión. Prevención y Mitigación; Febrero de 2018.

[41] Jang-Jaccard J, Nepal S. Una encuesta sobre amenazas emergentes en ciberseguridad. J Comput Syst Sci 2014; 80 (5): 973–93.

[42] Schneier B. Haga clic aquí para matar a todos: seguridad y supervivencia en un mundo hiperconectado. WW Norton & Company; 2018.

[43] Comiter M. Atacando la inteligencia artificial: la vulnerabilidad de seguridad de la ia y lo que los legisladores pueden hacer al respecto 2019.

[44] Dirección Nacional de Protección y Programas Oficina de Análisis Cibernético e Infraestructura. El futuro de las ciudades inteligentes: riesgo de infraestructura ciberfísica. Departamento de Seguridad Nacional de los Estados Unidos; Agosto de 2015.
[45] Babic B, Gerke S, Evgeniou T, Cohen IG. Algoritmos sobre bloqueo regulatorio en medicina. Science 2019; 366 (6470): 1202–4.
[46] Diez CW, Hong J, Liu CC. Detección de anomalías para la ciberseguridad de las subestaciones. IEEE Trans Smart Grid 2011; 2 (4): 865–73.
[47] Instituto Nacional de Estándares y Tecnología. Consideraciones para administrar los riesgos de privacidad y ciberseguridad de Internet de las cosas (IoT). Gaithersburg, MD; Junio de 2019.
[48] DR Jg, J. Rydning. La digitalización del mundo: del borde al núcleo Framingham, MA; Noviembre de 2018 [Disponible en: https://www.seagate.com/files/wwwcontent/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf.
[49] Administración de Drogas y Alimentos de los Estados Unidos. URGENTE / 11 Las vulnerabilidades de seguridad cibernética en un componente de software de terceros ampliamente utilizado pueden introducir riesgos durante el uso de ciertos dispositivos médicos. Comunicación de seguridad de la FDA; 1 de octubre de 2019 [Disponible desde,https://www.fda.gov/medical-devices/safety-communications/2019-sa fety-communications.
[50] Arute F, Arya K, Babbush R, Bacon D, Bardin JC, Barends R, et al. Supremacía cuántica utilizando un procesador superconductor programable. Nature 2019; 574 (7779): 505–10.
[51] Instituto Nacional de Normas y Tecnología. Criptografía post-cuántica; 03 de enero de 2017 [Disponible en:https://csrc.nist.gov/projects/post-quant um-cryptography.
[52] Centro de Política de Tecnología de la Información de la Universidad de Princeton. Implicaciones de la computación cuántica para la política de cifrado. Washington, DC: Grupo de trabajo de cifrado Carnegie; Abril de 2019.
[53] Consorcio de Innovación de Dispositivos Médicos. Informe de ciberseguridad de dispositivos médicos. Avanzar en la divulgación coordinada de vulnerabilidades; 2018.
[54] Administración de Drogas y Alimentos de los Estados Unidos. Formulario de notificación voluntaria en línea de MedWatch [Disponible en:https://www.accessdata.fda.gov/scripts/medwatch/index.cfm? action = reporting.home.
[55] Dameff CJ, Selzer JA, Fisher J, Killeen JP, Tully JL. Formación en ciberseguridad clínica mediante novedosas simulaciones de alta fidelidad. J Emerg Med 2019; 56 (2): 233–8.