JHI JOURNAL OF HEALTH INFORMATICS

Segurança da Informação na comunicação de dispositivos médicos: uma revisão *quasi*-sistemática

Information Security in the communication of medical devices: a quasi-systematic review

Seguridad de la información en la comunicación de dispositivos médicos: una revisión casi-sistemática

Guilherme Goldschmidt[1], Jéferson Campos Nobre[2], Rodrigo da Rosa Righi[2], Cristiano André da Costa[2]

RESUMO

Os dispositivos médicos - os quais são destinados a fins de diagnóstico, prevenção, controle ou tratamento de doenças - estão atualmente mais sofisticados em termos computacionais. Tais dispositivos apresentam novas funcionalidades como, por exemplo, comunicação sem fio. A comunicação sem fio é o mecanismo mais exposto a vulnerabilidades e serve como intermédio para agentes maliciosos realizarem ataques. Ademais, a literatura vigente apresenta diversas inconsistências nas informações fornecidas a respeito dos riscos de segurança e privacidade dos dispositivos médicos. O presente estudo tem como objetivo caracterizar a Segurança da Informação na comunicação de dispositivos médicos, a fim de identificar como a segurança é tratada. Para atingir o objetivo proposto, foi realizada uma revisão quasi-sistemática da literatura. Como resultado dessa revisão, foi possível caracterizar a Segurança da Informação na comunicação de dispositivos médicos. Assim, culminando na integração dos dados obtidos, servido de base para a comunidade acadêmica e gerando uma melhor compreensão da área.

Descritores: Segurança Computacional; Confidencialidade; Segurança de Equipamentos

ABSTRACT

Medical devices - which are intended for diagnosis, prevention, control or treatment of diseases - are currently more sophisticated in computational terms. Such devices present new features such as wireless communication. Wireless communication is the mechanism most exposed to vulnerabilities and serves as an intermediary for malicious agents to carry out attacks. In addition, the current literature presents several inconsistencies in the information provided regarding the safety and privacy risks of medical devices. The present study aims to characterize Information Security in the communication of medical devices in order to identify how safety is treated. To reach the proposed goal, a quasi-systematic review of the literature was performed. As a result of this review, it was possible to characterize an Information Security in the communication of medical devices. Thus, culminating in the integration of the data obtained, served as the basis for the academic community and generating a better understanding of the area.

Keywords: Computer Security; Confidentiality; Equipment Safety

RESUMEN

Los dispositivos médicos - los cuales están destinados a fines de diagnóstico, prevención, control o tratamiento de enfermedades - están actualmente más sofisticados en términos computacionales. Estos dispositivos presentan nuevas funcionalidades como, por ejemplo, comunicación inalámbrica. La comunicación inalámbrica es el mecanismo más expuesto a vulnerabilidades y sirve como intermedio para que los agentes maliciosos realicen ataques. Además, la literatura vigente presenta diversas inconsistencias en la información suministrada acerca de los riesgos de seguridad y privacidad de los dispositivos médicos. El presente estudio tiene como objetivo caracterizar la Seguridad de la Información en la comunicación de dispositivos médicos, a fin de identificar como la seguridad es tratada. Para alcanzar el objetivo propuesto, se realizó una revisión casi sistemática de la literatura. Como resultado de esta revisión, fue posible caracterizar la Seguridad de la Información en la comunicación de dispositivos médicos. Así, culminando en la integración de los datos obtenidos, servido de base para la comunidad académica y generando una mejor comprensión del área.

Descriptores: Seguridad Computacional; Confidencialidad; Seguridad de Equipos

[1] *Tecnólogo em Segurança da Informação pela Escola Politécnica, Universidade do Vale do Rio dos Sinos - UNISINOS, São Leopoldo (RS), Brasil.*
[2] *Professor da Escola Politécnica, Universidade do Vale do Rio dos Sinos - UNISINOS, São Leopoldo (RS), Brasil.*

Autor Coorespondente: **Guilherme Goldschmidt**
e-mail: **guigoldschmidt@edu.unisinos.br**

Artigo recebido: **02/08/2017**
Aprovado: **12/12/2018**

www.jhi-sbis.saude.ws

INTRODUÇÃO

Dispositivos médicos – os quais são destinados a fins de diagnóstico, prevenção, controle ou tratamento de doenças[1] – estão atualmente mais sofisticados em termos de aspectos computacionais. Além disso, dispositivos como a cápsula endoscópica sem fio[2] apresentam diversas novas funcionalidades como, por exemplo, mecanismos de comunicação sem fio[3]. A comunicação sem fio dos dispositivos médicos pode ser destacada como uma das principais funcionalidades[2] estando presente na maioria dos dispositivos. No entanto, a evolução das tecnologias de comunicação sem fio dos dispositivos médicos não foi acompanhada por um incremento da segurança[4]. Desta forma, a comunicação sem fio em dispositivos médicos é uma das tecnologias mais expostas a vulnerabilidades e serve como intermédio para agentes maliciosos realizarem ataques[4].

Dispositivos médicos estão muitas vezes relacionados a vida[3], assim a Segurança da Informação (SI) se faz necessária. No entanto, a segurança aplicada aos dispositivos médicos muitas vezes não se mostra eficaz[5]. Existem também muitas inconsistências nas informações fornecidas a respeito dos riscos de segurança e a privacidade dos dispositivos[6]. A SI implementada em dispositivos médicos é preocupante e por isso é constantemente tema de conferências e debates[7]. Além disso, com a crescente conectividade dos dispositivos médicos e a manipulação de informações sensíveis, o aumento dos ataques cibernéticos no setor da saúde vem se mostrando uma preocupação constante[8]. Ademais, as pesquisas atuais[9] não satisfazem as necessidades de integração das informações de segurança de forma que ainda existem lacunas nas informações. Essa falta da integração das informações sobre a área faz com que órgãos europeus continuem a investir em novas regras para tornar mais rígidas as avaliações de conformidade[10]. Órgãos de saúde realizam constantes eventos a fim de identificar os desafios da área[7], uma vez que falta integração das informações sobre os diferentes dispositivos, tecnologias e vulnerabilidades em dispositivos médicos.

O presente estudo, como forma de contribuir à SI no cenário de risco e de falta de integração de informações ao qual se encontram os dispositivos médicos, propõe caracterizar a SI na comunicação de dispositivos médicos. Desta forma, o estudo busca identificar como a segurança é tratada, conscientizar as partes interessadas e também agregar conteúdo para a comunidade acadêmica. Para atingir este propósito é realizada uma revisão *quasi*-sistemática da literatura[11], cujo planejamento, execução e resultados estão descritos neste documento. Assim, este estudo engloba os conhecimentos disponíveis sobre a SI na comunicação de dispositivos médicos, baseados em uma bibliografia pertinente.

Este trabalho está estruturado da seguinte maneira. A Seção 2 apresenta o método utilizado para a presente revisão. Na Seção 3, descreve-se o resultado das buscas da revisão, são analisados os documentos recuperados, extraídas as informações pertinentes e sintetizados os resultados obtidos. A Seção 4 tem como objetivo caracterizar a SI na comunicação de dispositivos médicos. Por fim, na Seção 5, são apresentadas as conclusões deste trabalho e as oportunidades de trabalhos futuros.

MÉTODO

Este estudo faz uso de uma revisão *quasi*-sistemática da literatura[11-13] e nesta seção é apresentado o método utilizado na execução desta revisão. São apresentadas também as estratégias de busca utilizadas, assim como os procedimentos seguidos pelos condutores da revisão.

O estudo em questão tem como propósito realizar uma caracterização da área, desta forma, não há o elemento comparação. Por consequência, como não há o elemento de comparação, esta revisão é chamada de *quasi*-sistemática, ainda que preserve o mesmo processo de uma revisão sistemática[13]. As subseções a seguir descrevem o processo utilizado nessa revisão. Esta revisão foi desenvolvida com base em modelos de revisões relevantes[11-14].

Questão de Pesquisa

A formulação da questão de pesquisa é a parte mais importante do desenvolvimento de uma revisão sistemática[15]. Desta forma, o estudo busca analisar experiências e publicações científicas com o propósito de caracterizar a comunicação sem fio de dispositivos médicos do ponto de vista da SI. Assim, foram definidas questões de pesquisa principais e secundárias. A questão de pesquisa principal foi refinada em várias questões secundárias a fim de prover uma melhor classificação e análise do assunto. As questões de pesquisa estão divididas em dois grupos: questão principal (QP) e questões secundárias (QS). Todas as questões de pesquisa estão listadas na Tabela 1.

Estratégia de Pesquisa

Esta etapa envolve dissolver as questões de pesquisa a fim de estruturar as expressões de busca. Para realizar este processo, foi utilizada a abordagem de estruturação de questão "*Population, Intervention, Comparison, Outcome*" (PICO)[13], onde a questão de pesquisa é subdivida em quatro elementos: população, intervenção, comparação e resultado[13]. O estudo em questão tem como propósito

Tabela 1 - Questões de Pesquisa

Grupo	Questão
Questão Principal (QP)	
QP	Qual é o estado da arte da SI na comunicação de dispositivos médicos?
Questões Secundárias (QS)	
QS1	Quais são os mecanismos de segurança aplicados a dispositivos médicos?
QS2	Quais são as vulnerabilidades e ameaças presentes em dispositivos médicos?
QS3	Quais tecnologias são utilizadas na comunicação sem fio entre dispositivos Médicos?

Fonte: Elaborado pelos autores, Julho. 2017.

realizar uma caracterização da área, desta forma, não utilizará do elemento comparação.

O elemento população busca abordar estudos, pesquisas ou artigos que apresentem experimentos e/ou descrevam as características da SI aplicadas a comunicação de dispositivos médicos. A intervenção busca identificar mecanismos de SI na comunicação de dispositivos médicos implantáveis e dispositivos médicos ativos. O estudo em questão tem como propósito realizar uma caracterização da área, desta forma, não há comparação. O elemento resultado tem como objetivo identificar o estado da arte em SI na comunicação de dispositivos médicos. Assim como, identificar quais são as tecnologias de SI implementados, quais são as vulnerabilidades presentes e os mecanismos de comunicação sem fio utilizados.

Para cada um dos elementos, "população" (P), "intervenção" (I) e "resultado" (R), foi definido uma combinação de palavras-chave. Estas palavras foram selecionadas levando em consideração o objetivo do estudo, o objeto de estudo e características de interesse. As palavras-chave selecionadas para cada um dos elementos estão elencadas abaixo.

P: (study OR research OR article OR paper OR analysis OR experiment OR experimentation OR test)

I: (mechanism OR system OR method OR technique OR process OR approach OR procedure OR technology) AND (security OR protection OR "information security" OR secure) AND (device OR appliance OR equipment OR instrument) AND (communication OR connection OR transmission) AND (medical OR health OR healthcare) AND (active OR implantable)

R: ("state of the art" OR highest)

Para tornar a busca mais sensível, os elementos foram relacionados com os operadores booleanos *AND* e *OR* entre termos[13]. Desta forma, resultando na seguinte estrutura: (P) *AND* (I) *AND* (R). A expressão geral de busca para a questão de pesquisa principal está presente na Caixa de Texto 1.

Seleção da Base de Dados

Para a seleção das bases de dados foram utilizados alguns critérios. Esses critérios incluíam disponibilizar seus conteúdos por meio da internet e fazer uso de um mecanismo de busca que permita a utilização de expressões lógicas. Também foram critérios, disponibilizar um mecanismo de pesquisa onde a busca fosse realizada no texto completo ou em campos específicos das publicações e garantir resultados únicos por meio da busca de um mesmo conjunto de palavras-chave. As bases de dados selecionadas são Engineering Village (Ei Compendex) e Scopus, disponíveis em http://www.engineeringvillage.org e http://www.scopus.com respectivamente. As bases citadas foram escolhidas em função das mesmas apresentarem uma diversidade de trabalhos em áreas correlatas fora da computação (por exemplo em comparação com o IEEE xplore e ACM Digital Library), o que aumenta a possibilidade de encontrarmos trabalhos relacionados na revisão da literatura.

Seleção de Artigos

O processo de seleção dos estudos foi organizado em quatro etapas que têm como objetivo registrar e descrever as ações dos pesquisadores, desde a consulta às bases de dados até a extração das informações dos estudos selecionados, conforme demostrado na Figura 1. A primeira etapa da seleção dos estudos é composta pela aplicação da expressão de busca às fontes selecionadas e pelo armazenamento e catalogação dos estudos no repositório de dados. Em seguida, na segunda etapa, dois revisores (GG e JC) avaliam os estudos por meio da leitura de seus resumos e da aplicação dos critérios de inclusão e exclusão que são apresentados na Tabela 2.

Na terceira etapa uma auditoria é realizada pelos demais revisores (RR e CA) a fim de validar se os critérios foram aplicados de forma correta e para realizar a inclusão ou exclusão de algum estudo que tenha ficado na situação de dúvida. A quarta etapa se resume na avaliação da lista de estudos após as triagens e no debate entre os revisores sobre as avaliações conflitantes. Caso haja algum impasse o estudo em questão deve ser incluído na lista. Apenas estudos que atenderam a ao menos um critério de inclusão (CI) e nenhum critério de exclusão (CE) foram considerados.

Como forma de reduzir o viés de seleção e informação, foram utilizadas medidas como a elaboração sistemática de uma expressão de busca, definição de critérios de avaliação dos estudos (Tabela III) e a extração sistemática das informações dos estudos selecionados. Assim, a seleção dos artigos se sucedeu de forma isométrica e seus conteúdos se provaram relevantes e completos a este estudo.

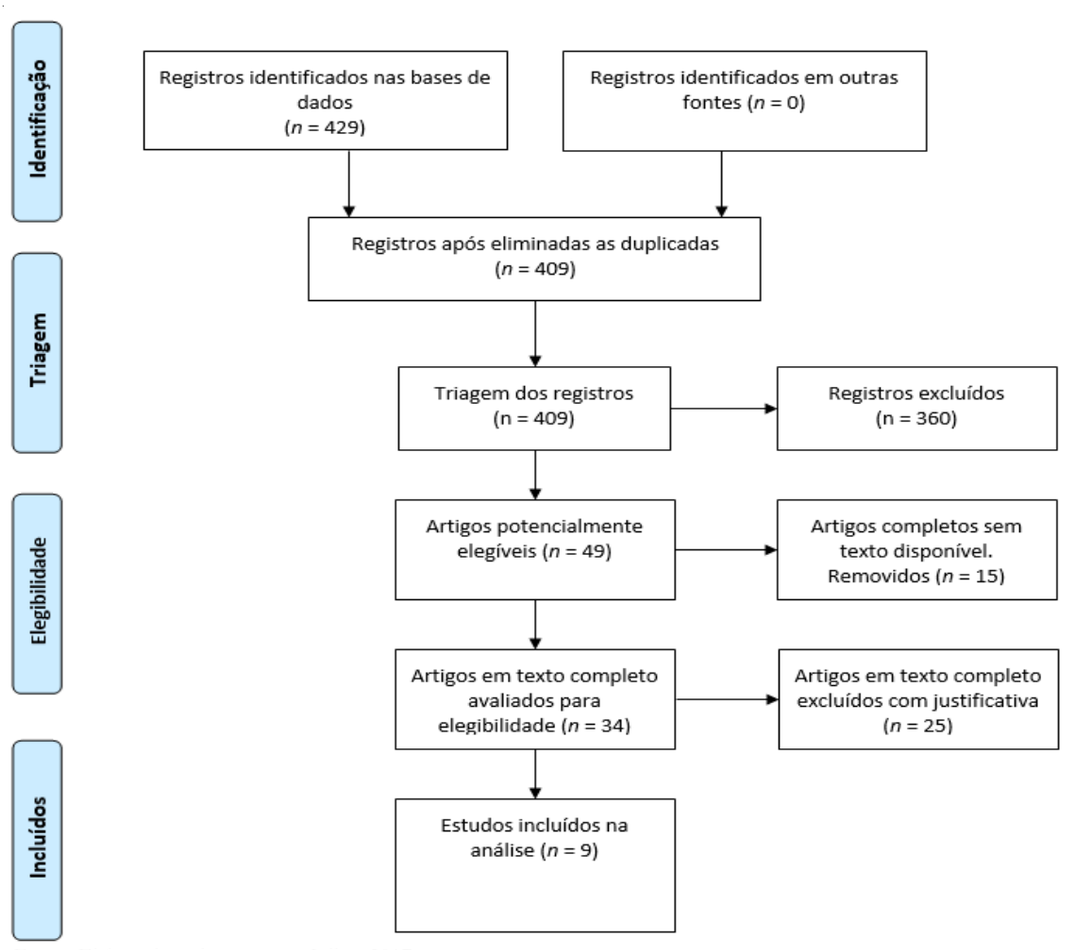
Amostra Final de Artigos

Esta seção descreve os resultados obtidos por meio da aplicação das expressões de busca, assim como da extração dos dados. A aplicação da expressão geral de busca foi realizada individualmente em cada base de dados no período de 13/11/2016 à 15/11/2016. Para as buscas foram adicionadas as limitações de pesquisa junto a expressão original, além das adaptações necessárias para

Caixa de Texto 1. Expressão de Busca

(study OR research OR article OR paper OR analysis OR experiment OR experimentation OR test) AND (mechanism OR system OR method OR technique OR process OR approach OR procedure OR technology) AND (security OR protection OR "information security" OR secure) AND (device OR appliance OR equipment OR instrument) AND (communication OR connection OR transmission) AND (medical OR health OR healthcare) AND (active OR implantable) AND ("state of the art" OR highest)

Fonte: Elaborado pelos autores, Julho. 2017.



Fonte: Elaborado pelos autores, Julho. 2017.

Figura 1 - Critérios de Inclusão e Exclusão de Estudos

Tabela 2 - Critérios de Inclusão e Exclusão de Estudos

Identificador	Questão
Critérios de Inclusão (CI)	
CI1	Documentos que descrevam o estado da arte da SI na comunicação de dispositivos médicos.
CI2	Documentos que relatem experiências em relação a comunicação de dispositivos médicos.
CI3	Documentos que apresentem os mecanismos de SI implementados em dispositivos médicos.
CI4	Estudos que descrevam as tecnologias aplicadas na comunicação sem fio de dispositivos médicos.
CI5	Documentos que descrevam vulnerabilidades e/ou ameaças presentes em dispositivos médicos.
Identificador	**Questão**
Critérios de Exclusão (CE)	
CE1	Serão eliminados os documentos que não estiverem escritos no idioma inglês.
CE2	Serão desconsiderados prefácios e apresentações de artigos de conferências.
CE3	Os documentos que não possuírem seu conteúdo disponível na íntegra por meio da internet serão desconsiderados.
CE4	Documentos que nitidamente tratarem de assuntos diferente ao abordado nesta revisão serão desconsiderados.
CE5	Caso o estudo trate de conceitos legais e não técnicos sobre o tema desta revisão o mesmo será desconsiderado.
CE6	Serão desconsiderados os estudos que relatem experiências em relação a comunicação de dispositivos médicos, mas não descreverem os resultados.
CE7	Só serão considerados estudos publicados entre 2006 e 2016, os demais serão desconsiderados.

Fonte: Elaborado pelos autores, Julho. 2017.

a pesquisa na específica base de dados. A busca foi realizada nos campos título, resumo e palavra-chave. Foram recuperados um total de 429 estudos. Desse total, 364 advindos da base Engineering Village e 65 da base Scopus.

Logo após a catalogação das pesquisas recuperadas por meio da expressão de busca foi realizada uma análise dos documentos e as duplicatas foram eliminadas, uma vez que um mesmo documento poderia estar presente em ambas as bases de dados. Nos casos de duplicidade, o estudo mais recente ou descritivo foi mantido. Desta forma, permaneceram um total de 409 estudos. Desses estudos, 352 são advindos da base Engineering Village e 57 estudos da base Scopus.

Após os processos de classificação dos estudos e eliminação de duplicatas, os estudos foram submetidos a dois filtros. Para o primeiro filtro, foram objetos de revisão os campos resumo e título dos estudos. Nesses campos foram aplicados os critérios de inclusão e exclusão e então com base nos resultados os documentos foram classificados. Desta forma, restaram um total de 49 estudos.

O segundo filtro consiste em uma avaliação mais detalhada dos estudos e para isso se faz necessária a leitura completa dos documentos. Entretanto alguns estudos não puderam ser recuperados completamente, uma vez que a base de dados não disponibiliza seus conteúdos completos. Então os artigos que não tiveram seus conteúdos completos recuperados foram removidos. Os estudos que tiveram seus conteúdos recuperados por completo foram lidos e avaliados novamente sobre os critérios de inclusão e exclusão.

Como resposta para as questões de pesquisa, foram encontrados 09 estudos que respondessem à questão principal (QP), assim como 08 estudos para a questão secundária (QS1), 03 estudos para a questão secundária (QS2) e 08 estudos para a questão secundária (QS3). O mesmo artigo pode responder a mais de uma questão de pesquisa. Os estudos selecionados estão apresentados na Tabela 3.

Após a extração das informações pertinentes, a Tabela 4 foi desenvolvida a fim de elencar palavras-chave que sintetizassem as ideias das questões de pesquisa, assim dividindo-as em colunas. A tabela foi organizada informando o autor do estudo, o dispositivo mencionado, as vulnerabilidades a ele identificadas, os mecanismos de segurança afetados e por fim os impactos na SI. Como forma de caracterizar a SI, foram utilizados quatro dos principais fundamentos de segurança. São eles a confidencialidade, integridade, disponibilidade e a autenticidade.

DISCUSSÃO

Neste estudo, procurou-se identificar artigos que permitissem uma visão clara da SI na comunicação de dispositivos médicos nos últimos anos. Esta pesquisa se propôs a destacar alguns dos estudos mais relevantes da área de acordo com critérios de seleção sistemáticos. A pesquisa procurou identificar vários aspectos comuns dos estudos respondendo a uma série de questionamentos de pesquisa. Como resultado, foi possível caracterizar a SI na comunicação de dispositivos médicos e identificar lacunas a serem pesquisadas, que representam desafios e questões que foram detectadas nos últimos anos. Essas questões de pesquisa são discutidas nas próximas subseções.

Dispositivo

Conforme o levantamento realizado e as informações resumidas na Tabela 4, pode-se verificar que são propostos vários dispositivos para as mais variadas funções como, por exemplo, dispositivos para diagnósticos[2] e dispositivos para tratamento de doenças[3]. Dentre estes dispositivos, podemos destacar os sensores corporais sem fio[18], os dispositivos médicos implantáveis[19-21] e a cápsula endoscópica sem fio[2] que representam a diversidade do uso da tecnologia na medicina e a sua representatividade no cotidiano das pessoas.

Com base na análise dos estudos mencionados na Tabela 4 é possível verificar como a tecnologia se tornou

Tabela 3 - Estudos Selecionados

Autores e Ano	Título do Estudo
Arsalan et al. (2013)[16]	Implantable intraocular pressure monitoring systems: Design considerations
Beck et al. (2011)[5]	Block cipher based security for severely resource-constrained implantable medical devices
Ciuti et al. (2016)[2]	Frontiers of robotic endoscopic capsules: a review
Darwish and Hassanien (2011)[17]	Wearable and implantable wireless sensor network solutions for healthcare monitoring
Moravejosharieh and Lloret (2016)[18]	Performance evaluation of co-located IEEE 802.15.4-based wireless body sensor networks
Rasmussen et al. (2009)[19]	Proximity-based access control for implantable medical devices
Seepers et al. (2014)[20]	Adaptive entity-identifier generation for IMD emergency access
Sejdić et al. (2013)[3]	Innovation and translation efforts in wireless medical connectivity, telemedicine and emedicine: A story from the RFID center of excellence at the university of pittsburgh
Strydis et al. (2013)[21]	A system architecture, processor, and communication protocol for secure implants

Fonte: Elaborado pelos autores, Julho. 2017.

Tabela 4 - Dados Extraídos Dos Estudos

Autor	Dispositivo	Vulnerabilidade	Mecanismo	Impacto na Segurança
Arsalan et al. (2013)[16]	Monitoramento de pressão intraocular elevada (IOPM)	Não possui nenhum mecanismo de segurança	Qualquer	Disponibilidade; Confidencialidade; Integridade; Autenticidade;
Beck et al. (2011)[5]	Sistema de alojamento artificial (AAS)	Informações em texto claro	Criptografia	Confidencialidade
		Não possui mecanismo de autenticação Não possui mecanismo de integridade	Autenticação; Criptografia;	Confidencialidade; Integridade; Autenticidade;
Ciuti et al. (2016)[2]	Cápsula Endoscópica sem fio (WCE)	Utiliza frequência de transmissão não protegida	Comunicação	Confidencialidade; Integridade; Disponibilidade
Darwish and Hassanien (2011)[17]	Redes corporais sem fio (WBAN)	Sem garantia de entrega de pacotes	Comunicação	Disponibilidade
		Ponto de falha no método de autenticação	Autenticação	Confidencialidade; Integridade; Disponibilidade
		Método de criptografia não eficiente	Comunicação	Confidencialidade
Moravejosharieh and Lloret (2016)[18]	Sensores corporais sem fio	Sem controle dos canais de transmissão	Comunicação	Disponibilidade
Autor	Dispositivo	Vulnerabilidade	Mecanismo	Impacto na Segurança
Rasmussen et al. (2009)[19]	Dispositivos médicos implantáveis (IMD)	Ponto de falha no controle de acesso	Autenticação	Integridade; Confidencialidade; Autenticidade;
		Não possui a blindagem adequada dos circuitos	Comunicação	Disponibilidade
Seepers et al. (2014)[20]	Dispositivos médicos implantáveis (IMD)	Chave única de acesso	Autenticação	Confidencialidade Disponibilidade; Autenticidade;
Sejdić et al. (2013)[3]	Dispositivo de gerenciamento de ritmo cardíaco (CRMDs)	Utiliza frequência de transmissão não protegida	Comunicação	Disponibilidade
Strydis et al. (2013)[21]	Dispositivos médicos implantáveis (IMD)	Comunicação sempre aberta	Comunicação	Disponibilidade
		Autenticação unilateral	Autenticação	Confidencialidade

Fonte: Elaborado pelos autores, Julho. 2017.

parte da medicina, estando presente em uma quantidade significativa de procedimentos, inclusive tornando-se essencial para alguns tratamentos médicos. Tratamentos como no caso do monitoramento de pressão intraocular elevada, onde a temperatura do olho é monitorada e controlada por meio de um microcomputador[16], só são possíveis com o constante incremento da tecnologia aos dispositivos médicos.

Vulnerabilidade

É possível verificar por meio da leitura dos estudos selecionados que a segurança de dispositivos médicos implantáveis ativos é objeto de pesquisa. No entanto, nenhum dos estudos selecionados mostrou a aplicação de mecanismos de segurança em dispositivos comerciais. Desta forma, é possível inferir que existem diversas vulnerabilidades às quais esses dispositivos podem estar sujeitos[21].

Os dispositivos médicos utilizam a radiofrequência para a troca de informações, assim se sujeitam a enviar as informações de um modo *broadcast*, ou seja, de uma maneira que qualquer leitor receba a comunicação. Um dos grandes desafios é estabelecer esta comunicação de forma que apenas o receptor correto consiga ter acesso aos pacotes enviados pelo dispositivo[21]. Esta mesma vulnerabilidade na comunicação é apresentada em dispositivos de monitoramento de pressão intraocular elevada[16].

Ao analisar as informações extraídas dos estudos selecionados, pode-se notar a escassez de documentos que fazem referência a vulnerabilidades em dispositivos médicos. No entanto, pôde-se constatar que dispositivos médicos estão sujeitos a vulnerabilidades como o envio de texto claro durante a comunicação[5], *Eavesdropping message* e Bateria DoS[21]. Grande parte das vulnerabilidades estão em questões como o canal de comunicação estar sempre escutando mesmo antes da autenticação e o dispositivo fazer uso de uma autenticação unilateral[21].

Mecanismo

A partir da análise da Tabela 4 e da leitura dos documentos recuperados é possível verificar que as áreas mais defasadas, se tratando de SI, são a comunicação e a autenticação. A SI é fundamental nos dispositivos médicos implantáveis, porém é possível verificar que mecanismos de SI não são prioridades no desenvolvimento destes equipamentos[16].

Diversos mecanismos de SI para dispositivos médicos implantáveis são propostos[19-21] como, por exemplo, mecanismos para assegurar que a interferência e o acesso

indevido a canais de comunicação sejam evitado[18]. Contudo, conforme pode-se averiguar nos estudos selecionados a aplicação comercial destes mecanismos não é sugerida.

A autenticação, assim como a criptografia, também foi objeto de análise nos documentos recuperados. Mecanismos para evitar ataques de repetição, que podem permitir acesso total do dispositivo apenas por falta de tratamento na troca de pacotes, são propostos[21] e prometem não trazer consumo considerável de energia. Outra solução apresentada para o controle de acesso de dispositivos médicos implantáveis é um sistema baseado em *ultrasonic distance-bounding* que permite o controle de recursos por meio da proximidade dos demais dispositivos[19]. Mecanismos de criptografia também são propostos, visam minimizar o ciclo de trabalho e fortalecer a segurança para informações altamente confidenciais, e se baseiam em criptografia em blocos com dois modos, um modo de fluxo e um modo de sessão[5].

Impacto na Segurança

Após uma leitura dos documentos verifica-se que vários dispositivos médicos comercialmente disponíveis não empregam qualquer forma de segurança. Sem segurança é possível alterar parâmetros de um dispositivo ou até mesmo desativá-lo. Por meio da Tabela 4, é possível verificar que os dispositivos médicos implantáveis possuem diversas vulnerabilidades que impactam os pacientes de diversas formas, sendo a mais grave delas a disponibilidade[20], pois o dispositivo pode estar ligado a funções vitais de um paciente e pode parar de operar. Assim como, os sistemas *Radio-Frequency IDentification* (RFID) que tem a capacidade de causar interferências em dispositivos de gerenciamento de ritmo cardíacos, desta forma o dispositivo de gerenciamento cardíaco pode não conseguir realizar sua função devido a interferência gerada[3].

Sobre a integridade, em um sistema de alojamento artificial, por meio da troca de dados entre sensores, existem vulnerabilidades que podem levar a captura de dados e a manipulação de mensagens por alguém não autorizado[5]. Através desta vulnerabilidade é possível ter acesso a todo um histórico de dados do paciente, revelando assim informações que podem ser utilizadas inclusive em atentados a vida. A confidencialidade é também parte preocupante em dispositivos médicos, vulnerabilidades como o envio de texto claro durante a comunicação[5] impactam diretamente na confidencialidade dos dados do paciente. Assim como a confidencialidade, a integridade das informações contidas e passadas pelos dispositivos possuem incidência menor, seu impacto a curto prazo é menor[20], porém também são dados encontrados na análise dos documentos recuperados nesta revisão *quasi*-sistemática. Já a autenticação apresenta fragilidades menos técnicas, entretanto ainda graves[5,19]. Por exemplo, através do uso de abordagens de credenciais secretas a autenticação pode ser fraudada, pois podem não haver garantias de que o médico esteja lendo o dispositivo esperado[19].

CONCLUSÃO

Este estudo teve como objetivo levantar e discutir as principais questões sobre a SI na comunicação de dispositivos médicos. Para responder às questões de pesquisa deste artigo, buscou-se primeiro sistematizar a informação que serviu como fonte para a pesquisa. Diferente das pesquisas atuais, a presente proposta foi capaz de caracterizar a SI na comunicação de dispositivos médicos por meio de uma busca de informações sistemática, leitura e classificação das informações. Assim, realizando um levantamento dos variados dispositivos médicos, seus mecanismos de segurança, suas vulnerabilidades computacionais e os impactos na segurança aos quais estão sujeitos. Desta forma, é possível afirmar que os mecanismos de SI apresentados nos estudos selecionados refletem o estado da arte da SI na comunicação de dispositivos médicos.

Além de responder as questões de pesquisa, foi possível classificar as informações. As respostas e classificações obtidas contribuem para a obtenção de uma integração de informações de SI em relação aos dispositivos médicos. Essa integração das informações acaba por identificar pontos importantes quanto a segurança que podem vir a ser objetos de estudos futuros, assim como agrega conteúdo sobre o assunto e pode ser utilizado de referência pela comunidade acadêmica. Pôde-se verificar que existem diversos mecanismos de SI para dispositivos médicos[19-21]. Além dos mecanismos foram identificadas diversas vulnerabilidades com grandes impactos aos dispositivos médicos. São propostos modelos[21] como medida para incrementar a segurança em dispositivos médicos. Contudo, os estudos selecionados não apontam indicações de uso comercial dessas tecnologias.

Estudos futuros podem seguir na resolução de problemas como a interferência nos sinais de rádio na comunicação dos dispositivos médicos. Outro ponto de atenção é na autenticação dos usuários. Embora já existam propostas de autenticação segura, ainda há pontos que necessitam de melhorias, como balanceamento entre a segurança e a comodidade dos usuários. Outro aspecto que pode servir como um estudo futuro é explorar a maneira com que as informações são enviadas e recebidas, usualmente em texto claro, o que torna a comunicação insegura. Ainda, revisões futuras podem incrementar bases de dados para a coleta de estudos, refinar as questões de busca e propor uma taxonomia das informações coletadas.

REFERÊNCIAS

1. Conselho da União Europeia. Directiva 93/42/CEE de 14 de Junho de 1993, relativa aos dispositivos médicos. J Oficial das Comunidades Européias. N. L 169/2; 1993.
2. Ciuti G, Caliò R, Camboni D, Neri L, Bianchi F, Arezzo A, et al. Frontiers of robotic endoscopic capsules: a review. J Microbio Robot. 2016;11(1):1-18.
3. Sejdiæ E, Rothfuss MA, Stachel JR, Franconi NG, Bocan K, Lovell MR, et al. Innovation and translation efforts in wireless

medical connectivity, telemedicine and emedicine: a story from the RFID center of excellence at the university of pittsburgh. Ann Biomed Eng. 2013 Sep;41(9):1913-25.
4. Souza B. Dispositivos médicos eletrônicos na mira dos hackers. [acesso em 2017 mai 18]. Disponível em: https://canalcienciascriminais.com.br/dispositivos-medicos-eletronicos-na-mira-dos-hackers/
5. Beck CA, Masny DB, Geiselmann WB, Bretthauer GA. Block cipher based security for severely resource-constrained implantable medical devices. Proceedings of the 4th International Symposium on Applied Sciences in Biomedical and Communication Technologies; 2011 Oct 26-29; Barcelona, Spain. p. 62.
6. Kramer DB, Baker M, Ransford B, Molina-Markham A, Stewart Q, Fu K, et al. Security and privacy qualities of medical devices: an analysis of FDA postmarket surveillance. PLoS One [Internet]. 2012;7(7):1-7. Available from: https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0040200
7. U.S Food & Drug. Public Workshop - Cybersecurity of medical devices: a regulatory science gap analysis. [cited 2017 jul 21]. Available from: https://www.fda.gov/MedicalDevices/NewsEvents/WorkshopsConferences/ucm549732.htm
8. Santos C. Relatório mostra as tendências de cibersegurança em IoT para 2017. [acesso em 18 mai 2017]. Disponível em: http://convergecom.com.br/tiinside/seguranca/tecnologia-seguranca/06/04/2017/9-tendencias-de-ciberseguranca-em-iot-para-2017/
9. Rios B, Butts J. Security evaluation of the implantable cardiac device ecosystem architecture and implementation interdependencies. WhiteScope; 2017. 27p.
10. Nadkarni I. Saúde: PE aprova regras para reforçar controle dos dispositivos médicos na UE. [acesso em 18 maio 2017]. Disponível em: http://www.europarl.europa.eu/news/pt/press-room/20170329IPR69055/saude-pe-aprova-regras-para-reforcar-controlo-dos-dispositivos-medicos-na-ue
11. Biolchini J, Mian PG, Natali ACC, Travassos GH. Systematic review in software engineering. System Engineering and Computer Science Department. Universidade Federal do Rio de Janeiro. Programa de Engenharia de Sistemas e Computação. RT–ES 679; 2005.
12. Magdaleno A, Werner CM, Araujo R de. Revisão quasi-sistemática da literatura: conciliação de processos de desenvolvimento de software [relatório técnico]. Rio de Janeiro: Universidade Federal do Rio de Janeiro (UFRJ). Programa de Engenharia de Sistemas e Computação; 2009.
13. Pai M, Mcculloch M, Gorman JD, Pai N, Enanoria W, Kennedy G, et al. Systematic reviews and meta-analyses: an illustrated, step-by-step guide. Natl Med J India. 2004 Mar-Apr;17(2):86-95.
14. Munzlinger E, Narcizo FB, Queiroz JER de. Protocolo de revisão sistemática [apresentação]. Universidade Federal de Campina Grande. Programa de Pós-Graduação em Ciência da Computação; 2012.
15. Kitchenham B. Procedures for performing systematic reviews. Department of Computer Science Keele University. TR/SE-0401, 2004.
16. Arsalan M, Ouda MH, Marnat L, Shamim A, Salama KN. Implantable intraocular pressure monitoring systems: design considerations. Proceedings of the International Microwave Workshop Series on RF and Wireless Technologies for Biomedical and Healthcare Applications (IMWS-BIO); 2013 Dez 9-11; Singapure: Curran Associates Inc.
17. Darwish A, Hassanien A. Wearable and implantable wireless sensor network solutions for healthcare monitoring. Sensors (Basel). 2001;11(6):5561-95.
18. Moravejosharieh A, Lioret J. Performance evaluation of co-located ieee 802.15.4-based wireless body sensor networks. Annals of Telecommunications. 2016; 71(9/10):425-40.
19. Rasmussen KB, Castelluccia C, Heydt-Benjamin TS, Capkun S. Proximity-based access control for implantable medical devices. Proceedings of the 16th ACM Conference on Computer and Communications Security; 2009 Nov 9-13; Chicago,IL. USA. p. 410-9.
20. Seepers RM, Strydis C, Sourdis I, De Zeeuw CI. Adaptive entity-identifier generation for imd emergency access. Proceedings of the First Workshop on Cryptography and Security in Computing Systems; 2014 Jan 20; Viena, Austria. p. 41-4.
21. Strydis C, Seepers RM, Peris-Lopez P, Siskos D, Sourdis I. A system architecture, processor, and communication protocol for secure implants. ACM Transactions on Architecture and Code Optimization (TACO). 2013 Dec;10(4):57.