V Simpósio de Iniciação Científica 2022
Ciência, Tecnologia e Inovação no Brasil

CATEGORIZAÇÃO DE VULNERABILIDADES DE SEGURANÇA EM SISTEMAS DE IOT

Fábio Piovani Viviani[1] (IC), Lina Maria Garcés Rodriguez (PQ)[1]
[1]*Universidade Federal de Itajubá.*

Palavras-chave: Cibersegurança. Internet das coisas. Internet das coisas na saúde. Vulnerabilidades.

Introdução

Na atualidade, a rápida expansão de dispositivos para a *Internet of Things* (*IoT* — em português, Internet das Coisas) na área da saúde, somada a uma necessidade de baratear e personalizar o acesso de um paciente aos cuidados com sua própria saúde, faz com que a Internet das Coisas desempenhe um papel cada vez mais presente dentro do gerenciamento médico (Habibzadeh et al., 2020). Com o surgimento da COVID-19, o desvanecimento das barreiras existentes entre uma pessoa e a virtualização de seus serviços em saúde foi acelerado ainda mais, devido às restrições impostas pela própria doença, que, na maioria das vezes, impediam o trânsito do paciente até seu respectivo médico (Kelly et al., 2020).

De acordo com Usak et al. (2019), não existem muitas pesquisas que acentuam os desafios encontrados ao realizar a integração entre um dispositivo *IoT* e o gerenciamento da saúde; dessa forma, a falta de documentação sobre a utilização de tais dispositivos, corrobora para a falha na implementação dos mesmos. Devido à arquitetura aberta de um sistema de Internet das Coisas, garantir a segurança desses sistemas se torna uma tarefa ainda mais árdua; sua arquitetura possui diversas propriedades que podem levar ao surgimento de falhas — tais como sua constante conexão com a internet (Jurcut et al., 2020) — colocando a privacidade do usuário em risco e elevando as necessidades de segurança dos dispositivos de *IoT* (Rizvi et al., 2018). Sendo assim, Habibzadeh et al. (2020) pontuam que a falta de cibersegurança em um componente IoT, além de oferecer risco à privacidade do usuário, em dispositivos voltados para a área médica também arrisca sua saúde e integridade física.

Este trabalho foca-se em auxiliar os engenheiros de software na criação de arquiteturas seguras para sistemas de *IoT*. Para isso, visa-se a investigação das possíveis vulnerabilidades de segurança de sistemas de Internet das Coisas e descrição de suas características e maneira como afetam um sistema. Busca também utilizar da *IoT* na saúde como forma de alerta, exemplificando possíveis consequências de uma cibersegurança pobre nesses ambientes; reforçando assim a necessidade de se atentar à tal área ao se desenvolver um projeto em Internet das Coisas. Dessa forma, o trabalho está orientado a melhorar a construção destes sistemas desde uma visão da engenharia de software, tendo a qualidade desses sistemas — e não somente a funcionalidade — como foco principal. Realizou-se uma revisão de literatura rápida; identificando, coletando e interpretando dados primários e secundários.

As seções posteriores do presente trabalho são divididas da seguinte maneira: a Seção 2 contém o marco teórico, onde os conceitos relevantes para este trabalho são apresentados; a Seção 3 detalha os métodos utilizados no desenvolvimento e planejamento do trabalho; a Seção 4 descreve os resultados obtidos a partir do planejamento e execução da revisão de literatura; a Seção 5 aborda trabalhos relacionados, contribuições do trabalho desenvolvido e validade do mesmo; a Seção 6 conclui o trabalho.

Metodologia

O objetivo deste trabalho é identificar e caracterizar os diversos tipos de vulnerabilidades de segurança para sistemas de IoT, assim como utilizar-se de um contexto de *IoT* na saúde para exemplificar os perigos de um ciberataque.

Para a identificação das vulnerabilidades, utilizou-se o método de Revisões Rápidas (Temple University, 2021), caracterizado por uma forma de síntese de evidências que podem fornecer informações mais oportunas para a tomada de decisões em comparação com as revisões sistemáticas padrões. As Revisões Rápidas são projetadas especialmente para atender a tópicos de pesquisa novos ou emergentes, atualizações de revisões anteriores ou tópicos críticos, para avaliar o que já se sabe sobre uma política ou prática usando alguns métodos de revisão sistemática (Temple University, 2021). O método de revisões rápidas foi escolhido no lugar da revisão sistemática padrão por seu caráter de urgência; sendo uma revisão que é executada de modo mais rápida, se enquadrou

melhor no tempo alocado para a atual pesquisa.

Nessa metodologia, o período destinado para revisão é de usualmente cinco semanas; entretanto, na presente pesquisa, utilizou-se de oito semanas para sua concretização. Selecionou-se, portanto, artigos, livros e literatura cinza — conteúdo não academicamente publicado, como relatórios técnicos — relevantes à temática de segurança na Internet das Coisas; coletaram-se e interpretaram-se os dados para entender a fundo os problemas por trás das vulnerabilidades encontradas e identificar as causas e consequências das referidas.

Para a realização da revisão, o processo foi dividido em etapas de acordo com as descrições providas por Dobbins (2017). Dobbins (2017) estabeleceu cinco diferentes etapas: definir uma questão prática; buscar evidências científicas; avaliar criticamente as fontes; sintetizar as evidências; identificar a possibilidade de aplicação e problemas ocasionados pela mesma para consideração final.

Resultados e discussão

A coleta dos resultados se deu através de buscas e seleções por trabalhos pertinentes, realizadas por duas pessoas ao longo de um período de oito semanas. Posteriormente, as fontes sintetizadas, de acordo com a metodologia descrita na seção anterior, foram analisadas a fim de se chegar nos resultados compreendidos na atual seção.

Uma vulnerabilidade em um sistema, quando detectada pela pessoa errada, pode ser utilizada de modo a obter acesso desautorizado em um sistema e, posteriormente, consultar ou manusear dados que lá se encontram com intenções maliciosas (Agbamoro, 2019). Ao adentrarmos um contexto de *IoT* na área da saúde, os riscos advindos de tal invasão assumem um aspecto ainda mais perigoso devido à natureza dos dados; provenientes de um contato direto com a saúde de pacientes (Cynerio, 2022). Em conformidade com Cynerio (2022), quanto mais próximo um dispositivo de *IoT* se localiza do leito de um paciente, maiores são os riscos que aquele dispositivo representa caso seja invadido; visto que se encontra intimamente relacionado ao estado vital do paciente.

Desse modo, o presente trabalho buscou exemplos de ciberataques ocorridos em tal contexto para alertar pesquisadores e desenvolvedores da tecnologia da informação quanto à repercussão negativa que uma invasão pode adquirir.

Uuma vulnerabilidade não tratada pode abrir brechas em um sistema de *IoT*, colocando-o à disposição de invasões (Agbamoro, 2019). Se faz observável, através dos exemplos apresentados que, tais invasões, quando inseridas em determinados contextos, como em um projeto de Internet das Coisas na área da saúde, comprometem mais do que a privacidade do usuário, mas também sua vitalidade (Cynerio, 2022). Portanto, o presente trabalhou buscou utilizar-se desses casos para exemplificar uma máxima negativa das consequências de um ciberataque em um sistema de *IoT*. Posto isso, é imperativo reforçar que o nível de atenção prestado à segurança de um sistema de Internet das Coisas deve ser maior do que em qualquer outro tipo de sistema (Ogonji et al., 2020).

A natureza expositória de um sistema *IoT*, sempre conectado à internet e sempre aberto à comunicação, o torna mais suscetível a ter suas vulnerabilidades exploradas (Jain et al., 2020). Por conseguinte, é necessário que essas vulnerabilidades sejam mitigadas antes mesmo do dispositivo ser exposto a rede da qual fará parte; desse modo, o presente trabalho se predispôs a realizar uma análise de literatura científica atrás de vulnerabilidades comuns e conhecidas dentro da Internet das Coisas e as sumarizou na atual sessão. O objetivo é servir de fonte de consulta de vulnerabilidades de segurança para futuros pesquisadores e engenheiros de *software*, de modo que, a partir do presente documento, possam elaborar estratégias para lidar com as mesmas.

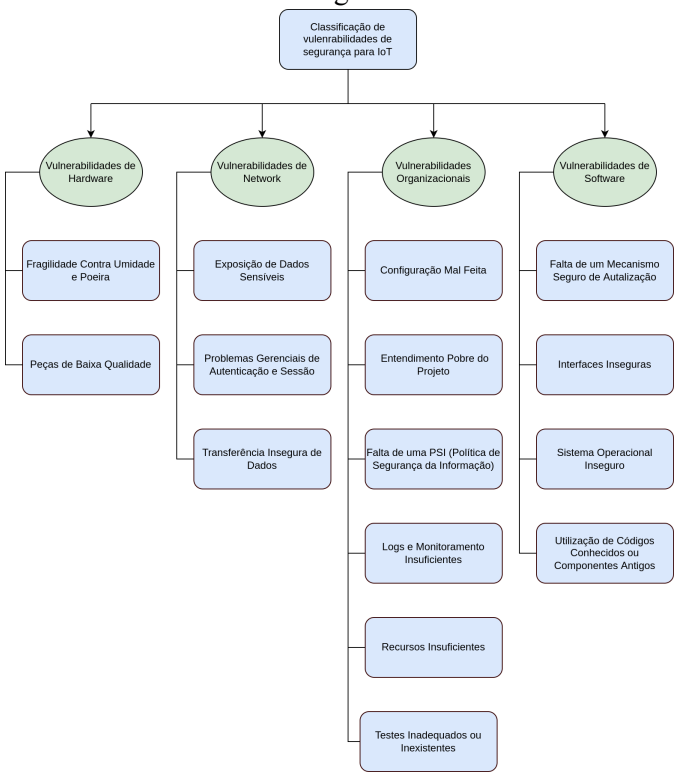
É necessário salientar que as vulnerabilidades dispostas na pesquisa atual foram apenas aquelas que se mostraram mais corriqueiras dentro do ambiente Internet das Coisas, de modo que o presente texto sirva como apoio às equipes desenvolvedoras ao realizarem revisões de segurança; buscando assim proporcionar um auxílio no que tange a mitigação dessas vulnerabilidades e do impacto que as mesmas teriam ao serem exploradas — principalmente ao se considerar a Internet das Coisas na saúde. Posto isto, é fundamental evidenciar que as vulnerabilidades aqui encontradas se aplicam a um contexto geral de *IoT* para prestar um referencial independente da área.

As vulnerabilidades encontradas na revisão de literatura tiveram sua categorização realizada em anuência às categorias propostas por Agbamoro (2019) — sendo as mesmas: Vulnerabilidade de *Hardware*; Vulnerabilidade de *Network*; Vulnerabilidade Organizacional; Vulnerabilidade de *Software*.

Ao se categorizar uma vulnerabilidade encontrada nos estudos primários, foi-se efetuada uma tentativa de adequar tal fragilidade à categoria que julgou-se mais adequada. Entretanto, por se tratar de uma questão subjetiva, algumas vulnerabilidades podem aparentar um enquadramento viável em outras

categorias; assim como também é possível encontrar na literatura vulnerabilidades semelhantes compreendidas em outras categorias por diferentes autores, como nos trabalhos de Hudson e Clark (2021) e Agbamoro (2019).

Figura 1 – Vulnerabilidades comuns de segurança para *IoT* de acordo com suas categorias.



Faz-se necessário o entendimento de que vulnerabilidades diferentes — inclusive as compreendidas em categorias diferentes — não são excludentes; podendo não só coexistirem, como estarem intimamente relacionadas, sendo uma vulnerabilidade uma possibilitadora ou até causa direta da outra. Para uma melhor representação das categorias e suas relações, foram elaborados dois diagramas, retratados nas Figuras 2 e 3, nos quais se tenta elucidar visualmente relações entre as vulnerabilidades listadas. Torna-se importante salientar novamente que a classificação apresentada é subjetiva à interpretação dos autores e pode variar levemente dependendo do contexto de cada sistema de *IoT*.

Ressalta-se que as vulnerabilidades atribuídas a outras através de uma relação de causa-consequência são apenas perspectivas; tais vulnerabilidades podem, ou não, ter relação com tais causas. Nas figuras propostas, as relações abordadas foram divididas em duas categorias: causadoras, compreendendo aquelas vulnerabilidades das quais sua existência pode diretamente acarretar na existência de outra; possibilitadoras, relações das quais a presença de uma vulnerabilidade possibilita um ambiente para que a existência de outra seja favorável, mas não necessariamente é sua causa direta.

Figura 2 – Relações causadoras entre as vulnerabilidades listadas

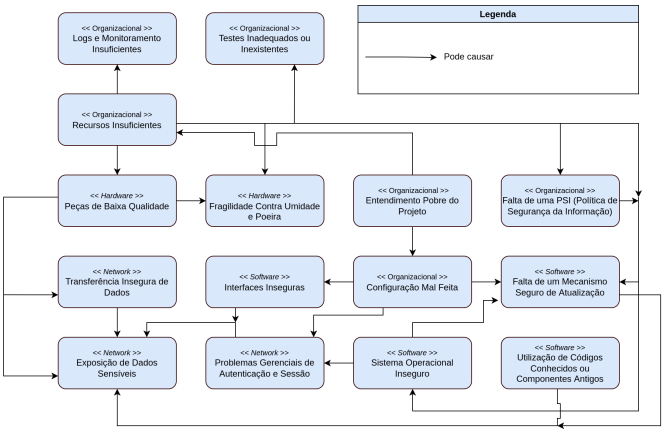
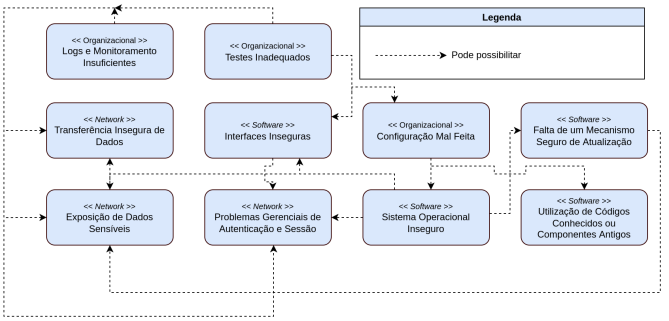


Figura 3 – Relações possibilitadoras entre as vulnerabilidades listadas



Conclusões

A atual pesquisa busca salientar a importância de se atentar à segurança de um sistema em Internet das Coisas através do assentamento de uma discussão quanto às consequências de um ciberataque em dispositivos integrados à saúde; contexto onde uma invasão pode custar a vida de uma, ou mais, pessoas. Buscou-se utilizar-se desse contexto para evidenciar uma máxima negativa em decorrência da elaboração de um sistema não seguro, ou seja, pretendeu-se dispor de tais dispositivos para definir uma circunstância onde tornasse claro as conclusões negativas que um ciberataque pode alcançar; apropriando-se de ataques reais para exemplificar tais negativas.

No atual trabalho, deseja-se que a síntese dos problemas encontrados sirva como diretriz para engenheiros de *software* e pesquisadores ao elaborarem seus próprios sistemas; é almejado que a pesquisa sirva

para nortear os mesmos ao realizarem revisões de segurança em seus produtos e apoie-os na elaboração de estratégias para mitigar tais vulnerabilidades aqui listadas.

Com a ascensão da Internet das Coisas dentro da sociedade contemporânea, obteve-se também um crescimento no número de ataques realizados nesse ambiente; com isso, observou-se uma necessidade por um maior cuidado ao lidar com a cibersegurança. Em um contexto *IoT*, os desafios para garantir a segurança e privacidade dos dados e dos usuários são ainda maiores do que os de um sistema de arquitetura fechada (Ogonji et al., 2020).

Posto isso, dentre a literatura revisada constituinte do assunto em questão não encontrou-se pesquisas que se prestassem a realizar uma listagem de quais são as características que, dentro de Internet das Coisas, mais frequentemente expõem os sistemas à riscos que desafiar a segurança do mesmo; levando a integridade para o caminho oposto do necessário, conforme citado no parágrafo anterior.

Considerando o problema citado, o presente trabalho procurou abordar tal levantamento. Deste modo, realizou-se uma sumarização e categorização das vulnerabilidades que tem maior incidência em sistemas de Internet das Coisas e acabam, por consequente, expondo-o a ataques e invasões.

Espera-se que a sumarização referida possa servir de base para futuras pesquisas ou que seja utilizada por desenvolvedores como uma métrica de segurança ao desenvolver seus próprios sistemas de Internet das Coisas.

Em suma, espera-se que a pesquisa realizada tenha condição de, por si só, auxiliar na manutenção da segurança em sistemas de Internet das Coisas, norteando engenheiros de software que a consultem; mas também possa servir de base para futuras pesquisas que resultem em trabalhos que amparem ainda mais o desenvolvimento de sistemas. De todo modo, deseja-se contribuir positivamente para o progresso de uma internet mais segura e confiável, garantindo mais integridade e proteção a todos os envolvidos.

Agradecimento

Agradeço à minha família e aos meus amigos, que me apoiaram durante todo o processo; agradeço à minha orientadora, que me deu toda a orientação e iluminação necessária; e, por último, agradeço a CNPq por disponibilizar os recursos necessários para a pesquisa prosseguir.

Referências

AGBAMORO, Michael Ogechi. Software Testing, Data Security and GDPR. Faculty of Technology, Natural sciences and Maritime Sciences, p. 61, 2019.

CYNERIO. The State of Healthcare IoT Device Security 2022. A Cynerio Research Report, p. 1-18, 2022.

DOBBINS, Maureen. Rapid Review Guidebook:: Steps for conducting a rapid review. The National Collaborating Center for Methods and Tools, v. 1, 2017.

HABIBZADEH, H. et al. A Survey of Healthcare Internet of Things (HIoT): A Clinical Perspective. IEEE Internet of Things Journal, v. 7, n. 1, p. 53-71, 2020.

HUDSON, Florence; CLARK, Chris. Wearables and Medical Interoperability: The Evolving Frontier. IEEE COMPUTER SOCIETY, p. 86-90, 2021.

JAIN, Neeraj Kumar; SAINI, Rajesh Kumar. Security Vulnerabilities in the IoT. Privacy and Data Security in the IoT, p. 93-114, 2020.

JURCUT, A. D.; RANAWEERA, P.; XU, L. Introduction to IoT Security. IoT Security: Advances in Authentication, p. 27-64, 2020.

KELLY, J. T. et al. The Internet of Things: Impact and Implications for Health Care Delivery. Journal of Medical Internet Research, v. 22, n. 11, 2020.

OGONJI, Mark; OKEYO, George; WAFULA, Joseph Muliaro. A survey on privacy and security of Internet of Things. Computer Science Review, p. 1-19, 2020.

RIZVI, S. et al. Securing the Internet of Things (IoT): A Security Taxonomy for IoT. IEEE Computer Society, p. 163-168, 2018.

TEMPLE UNIVERSITY. Systematic Reviews and Other Review Types. 2021. Disponível em: https://guides.temple.edu/c.php?g=78618&p=4156608. Acesso em: 28 fev. 2022.

USAK, M. et al. Health care service delivery based on the Internet of things: A systematic and comprehensive study. International Journal of Communication Systems, 2019.