Utilização de ontologias na avaliação de segurança cibernética na Internet das coisas: uma revisão sistemática de literatura

Mauricio Vianna de Rezende
Doutor em Sistemas de Informação e Gestão do Conhecimento pela Universidade FUMEC (FUMEC) - Brasil. Gerente de Engenharia do Produto. Responsável pela Integração de Arquiteturas Eletrônicas e Integração Veicular, liderando a Fábrica de Software da FCA (FIAT Chrysler Automobiles) e desenvolvimento do padrão AUTOSAR para o mercado LATAM.
http://lattes.cnpq.br/9759100648183157
https://orcid.org/0000-0003-3223-279X
E-mail: rezende.vianna@gmail.com

Rodrigo Moreno Marques
Pós-Doutorado pela Faculdade de Educação (UFMG) - Brasil. Pós-Doutorado pela University of London (UL) - Inglaterra. Doutor em Ciências da Informação pela Universidade Federal de Minas Gerais (UFMG) – Brasil, com período sanduíche em California State University - Estados Unidos. Professor da Universidade Federal de Minas Gerais (UFMG) – Brasil.
http://lattes.cnpq.br/4390865555343440
https://orcid.org/0000-0002-6320-4874
E-mail: rodrigomorenomarques@yahoo.com.br

Fernando Silva Parreiras
Pós-Doutorado pela Pontifícia Universidade Católica do Rio de Janeiro (PUC-Rio) - Brasil.
Doutor em Ciência da Computação pela Universität Koblenz-Landau (UNI-KOBLENZ-L) - Alemanha.
Professor e coordenador do Programa de Pós-Graduação em Sistemas de Informação e Gestão do Conhecimento da Universidade FUMEC (FUMEC) - Brasil.
http://lattes.cnpq.br/3564597309576489
https://orcid.org/0000-0002-9832-1501
E-mail: fernando.parreiras@fumec.br

Data de submissão: 17/10/2019. Data de aceite: 06/01/2021. Data de publicação: 10/12/2021.

RESUMO

A avaliação de segurança cibernética tornou-se crítica no desenvolvimento de dispositivos da Internet das Coisas (IoT – *Internet of Things*) e dos CPS (*Cyber Physical Systems*) automotivos em vários domínios de aplicação. A abordagem da avaliação de segurança cibernética suportada por ontologias é um caminho promissor para lidar com questões multidisciplinares e de diferentes domínios de conhecimento. Este artigo apresenta uma Revisão Sistemática da Literatura (RSL) com o objetivo de levantar as abordagens e aplicações empregadas em pesquisas que discutiram o uso de ontologias em avaliação de segurança cibernética em IoT e CPS automotivos. O resultado da RSL revela como ontologias têm sido empregadas na avaliação de segurança cibernética. Desse modo, são apresentadas as principais estratégias de avaliação em segurança cibernética, com foco na mitigação de vulnerabilidades, suportadas por ontologias, bem como as bases de conhecimento de padrões de ataques e vulnerabilidades que exploram as fraquezas cibernéticas conhecidas. Por fim, são trazidas à luz as principais métricas utilizadas durante o processo de avaliação em segurança cibernética relatadas na literatura acadêmica.

Palavras-chave: Segurança cibernética automotiva. Ontologia de avaliação em segurança cibernética. Ontologia.

Use of ontologies in cybersecurity assessment: a systematic literature review

ABSTRACT

The cybersecurity assessment has become critical in the development of the Internet of Things (IoT - Internet of Things) and automotive CPS (Cyber-Physical Systems) devices in various application domains. The cybersecurity assessment approach supported by ontologies is a promising way to deal with multidisciplinary issues and from different knowledge domains. This article presents a Systematic Literature Review with the objective of surveying (SLR) intending to survey the approaches and applications used in researches that discussed the use of ontologies in cybersecurity assessment in IoT and automotive CPS. The SRL results reveal how ontologies have been used to assess cybersecurity. The results also present the main cybersecurity assessment strategies supported by ontologies, the knowledge bases of attack and vulnerability patterns that exploit known cyber weaknesses, and the main metrics used during the cybersecurity assessment, reported in according to the academic literature.

Keywords*: Automotive Cybersecurity. Cybersecurity Ontology. Ontology.*

Uso de ontologías en la evaluación de ciberseguridad: una revisión sistemática de la literatura

RESUMEN

La evaluación de ciberseguridad se ha vuelto crítica en el desarrollo de Internet de las cosas (IoT - Internet of Things) y dispositivos automotrices CPS (sistemas ciberfísicos) en varios dominios de aplicación. El enfoque de evaluación de ciberseguridad respaldado por ontologías es una forma prometedora de abordar problemas multidisciplinarios y de diferentes dominios del conocimiento. Este artículo presenta una revisión sistemática de la literatura con el objetivo de realizar encuestas (SLR) con la intención de encuestar los enfoques y aplicaciones utilizados en investigaciones que analizaron el uso de ontologías en la evaluación de ciberseguridad en IoT y CPS automotriz. Los resultados de SRL revelan cómo se han utilizado las ontologías para evaluar la ciberseguridad. Los resultados también presentan las principales estrategias de evaluación de ciberseguridad respaldadas por ontologías, las bases de conocimiento de los patrones de ataque y vulnerabilidad que explotan las debilidades cibernéticas conocidas, y las principales métricas utilizadas durante la evaluación de ciberseguridad, informadas de acuerdo con la literatura académica.

Palabras clave*: Ciberseguridad automotriz. Ontologia de la Ciberseguridad. Ontología.*

INTRODUÇÃO

A IoT (*Internet of Things*) é formada por um conjunto de dispositivos de computação inter-relacionados com máquinas mecânicas e digitais fornecidas com identificadores exclusivos. Esse tipo de sistema tem a capacidade de interagir por meio de dados digitais em uma rede sem exigir interação homem-homem ou homem-máquina (HAMMONS; KOVAC, 2019). E, mais especificamente, a aplicação do IoT no mundo automotivo – com a integração de CPS (*Cyber Physical Systems*)[1], e a Internet, que possibilita a conexão do mundo virtual ao físico com a finalidade de resolver problemas complexos e explorar novas tecnologias no desenvolvimento da IoT e dos CPS – fomenta não somente a criação de novas tecnologias, mas também a aceleração do ciclo de inovação tecnológica (ALI; HONG, 2018).

Um dos mais importantes desafios para a adoção da IoT e dos CPS vem da própria heterogeneidade das soluções empregadas para conexão à Internet e das ameaças que surgem quando esses sistemas são expostos a essa rede de computadores. Assim, proteções em cibersegurança ganham destaque tanto no âmbito dos sistemas legados como dos novos sistemas (MOZZAQUATRO *et al.*, 2018).

Com a rápida expansão da IoT e dos dispositivos CPS, abrem-se novas e diversificadas perspectivas de usos dessas tecnologias, incluídas no desenvolvimento, por exemplo. das *smart cities*, dos *smart grids*, aplicações nos setores automotivo e de saúde. Estamos diante, portanto, de um campo multidisciplinar em que a adequada representação do conhecimento se torna imprescindível para garantir a construção de artefatos de softwares que resolvam problemas relativos aos dispositivos IoT, como a heterogeneidade de soluções e de protocolos de comunicação, e que minimizem os riscos ligados à cibersegurança nesse contexto (IBARRA-ESQUER *et al.*, 2017).

Dentro do universo dos CPS, destacam-se os CPS automotivos, que, integrados aos sistemas do veículo, se conectam à Internet e comandam sistemas físicos do automóvel. Esses CPS permitem o controle ativo sobre elementos reais do veículo e estão sujeitos às ameaças cibernéticas. Consequentemente, a cibersegurança, nesses dispositivos, envolve, além de dados privativos, a segurança física dos ocupantes do veículo (ABDULKHALEQ *et al.*, 2017). CPS automotivos e IoTs conectados à Internet, estão sujeitos a uma maior exposição a riscos de penetração maliciosa. Em 2014, mais da metade dos usuários de veículo se mostraram preocupados com a possibilidade de o carro ser manipulado por hackers quando o automóvel estiver conectado à Internet. Além disso, mais de 30% dos brasileiros rejeitam a ideia de carros conectados em razão do risco de perda de privacidade (HANNON *et al.*, 2018).

Soluções baseadas em ontologias têm sido empregadas para enfrentar problemas relativos à cibersegurança e à preservação da privacidade em dispositivos conectados à IoT (ALAM; CHOWDHURY; NOLL, 2011; FICCO, 2013; TAO *et al.*, 2018), bem como para gerir riscos (análise, avaliação e mitigação de riscos) envolvidos no processo de desenvolvimento desses dispositivos e de análise de cibersegurança com o foco na mitigação de vulnerabilidades (EKELHART; FENZ; NEUBAUER, 2009).

Diante disso, o objetivo deste artigo é discutir o emprego de ontologias para avaliação de cibersegurança e as abordagens que o tema tem recebido na literatura acadêmica. Pressupõe-se que avaliações de cibersegurança suportadas por ontologias são uma forma promissora de enfrentar os desafios da proteção de sistemas contra ameaças.

Para alcançar o objetivo proposto, foi feita uma revisão sistemática de literatura (RSL), utilizando o método de Kitchenham *et al.* (2009), com

[1] O termo Cyber Physical Systems compreende componentes digitais, analógicos, físicos e humanos em interação, projetados para funcionar por meio de integração física e lógica. Os CPS são originários da indústria de manufatura, como, por exemplo, robôs industriais que detectam seu ambiente e atuam de acordo com respostas programadas. Os CPS são aplicados em muitas áreas, incluindo saúde, assistência, sistemas de transporte inteligentes, sistema de resgate, vigilância e monitoramento.

abordagem baseada em evidências. Como primeiro passo do método, foram definidas questões a serem respondidas pela revisão sistemática. A recuperação e a seleção de artigos foram feitas por meio de chaves de busca direcionadas pelas questões de pesquisa e de critérios que permitiram a definição da relevância de cada artigo. O resultado da RSL revela como ontologias têm sido empregadas para avaliação de cibersegurança. Desse modo, são apresentadas as principais estratégias de avaliação em cibersegurança suportadas por ontologias e as bases de conhecimento de ataques e vulnerabilidades no âmbito da cibersegurança, além, por fim, das principais métricas de avaliação em cibersegurança relatadas na literatura acadêmica.

Na próxima seção deste artigo, é tecida uma breve discussão sobre ontologias e suas aplicações em cibersegurança. Na seção 3, é descrito o protocolo da revisão sistemática de literatura realizada. Na quarta seção, são analisados resultados encontrados, para que, na última seção, sejam apresentadas as considerações finais deste trabalho.

ONTOLOGIAS, TAXONOMIAS E SEGURANÇA DA INFORMAÇÃO

Segundo Gruber (1993), ontologia é a representação formal de uma conceitualização compartilhada. Almeida (2006) enriquece a definição do termo ao explicar que o estudo de ontologias é caracterizado como um ramo de pesquisa que propõe alternativas para representação do conhecimento através de uma série de formalismos capazes de representar conceitos, relações entre os conceitos e a semântica de um domínio do conhecimento que, por intermédio de declarações lógicas, podem ser manipuladas por um sistema computacional.

Ontologias oferecem a possibilidade de representar, organizar e desenvolver conjuntos complexos de conhecimento em diferentes áreas do conhecimento. Por meio das ontologias, são criados vocabulários que permitem que sejam feitas inferências a serem processadas mediante raciocinadores automáticos (ALMEIDA, 2013).

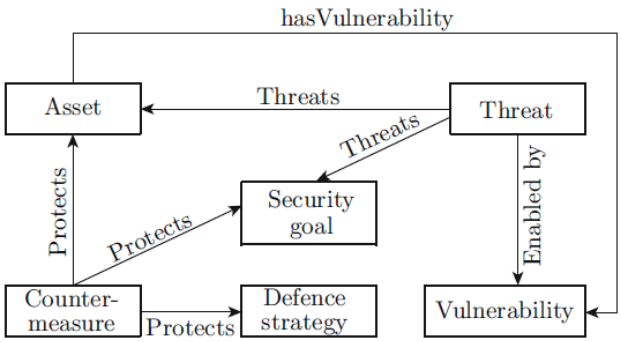
A estrutura oferecida pela ontologia pode ser entendida como uma representação formal e hierárquica de conceitos que se inter-relacionam em um domínio de conhecimento específico. Componentes comuns de uma ontologia são indivíduos, instâncias ou objetos, classes (conjuntos, coleções, conceitos, classes em programação, tipos de objetos, ou tipos de coisas), propriedades (aspectos, atributos, características, características ou parâmetros dos objetos e classes) e relações (maneiras pelas quais classes e indivíduos podem estar relacionados uns aos outros). Uma vez desenvolvida, esta estrutura abstrata permite ao usuário descrever uma estrutura de domínio do conhecimento, coletando sinônimos, capturando hierarquias como nas taxonomias, estabelecendo relações entre classes e indivíduos (KHAZAI *et al.*, 2014).

Van Rees (2003) define a taxonomia como uma estrutura hierárquica para auxiliar o processo de classificação de informações. Nas taxonomias, em geral, as informações são principalmente textuais, e o objetivo principal das taxonomias é sistematizar uma gama de vários elementos em uma estrutura hierárquica.

É importante distinguir as taxonomias das ontologias. Taxonomias são consideradas uma ontologia simples (MCGUINNESS, 2003), as ontologias são mais aprimoradas do ponto de vista semântico. Nas taxonomias preocupa-se com o desenvolvimento de categorias, inserção e recuperação da informação, enquanto nas ontologias o objetivo é o desenvolvimento de um consenso linguístico do domínio de conhecimento, levando em consideração, além dos relacionamentos taxonômicos adotados na ordenação de classes e subclasses, outros tipos de relações semânticas, como as de associação, derivadas da explicitação das características dos conceitos (VITAL; CAFÉ, 2011).

Herzog, Shahmehri e Duma (2007), ao proporem uma ontologia baseada em OWL[2] para segurança da informação, definiram componentes clássicos adotados em gestão de risco: ativos (*assets*), ameaças (*threats*), contramedidas (*countermeasures*), vulnerabilidades (*vulnerabilities*) e suas relações (figura 1). A ontologia proposta pelos autores, disponibilizada abertamente, pode ser usada como um vocabulário geral, roteiro e dicionário extensível do domínio da segurança da informação. Com sua ajuda, os usuários podem adotar uma linguagem comum com definição de termos e relacionamentos. Além disso, ela é útil para raciocinar sobre relacionamentos entre suas entidades, como, por exemplo, ameaças e contramedidas. A referida ontologia ajuda a responder a perguntas como: Quais contramedidas podem detectar ou impedir a violação da integridade dos dados?

Figura 1 − Principais classes e relacionamentos da Ontologia de Herzog, Shahmehri e Duma (2007) e os componentes clássicos de uma avaliação de risco



Fonte: Herzog, Shahmehri e Duma (2007).

Esforços similares feitos em CPS automotivos resultaram na norma SAE J3061 (SOCIETY OF AUTOMOTIVE ENGINEERS, 2016), que instituiu um guia para tratar requisitos de segurança cibernética e avaliar riscos. A norma SAE J3061 utiliza referências em cibersegurança da Internet, redes de computadores e dispositivos IoT como ponto de partida.

A SAEJ3061 apresenta um guia de avaliação para CPS automotivos e fornece informações e princípios de alto nível para as organizações do setor automotivo identificarem e avaliarem ameaças em cibersegurança, bem como para projetarem sistemas menos vulneráveis à ameaças e ataques (MACHER *et al.*, 2016). Nota-se que a referida norma não apresenta uma ontologia do conhecimento em cibersegurança para o domínio automotivo. Apesar de a norma representar o melhor esforço já alcançado para a área de cibersegurança em CPS automotivos, torna-se necessário que os engenheiros de requisitos e os engenheiros de segurança tenham o conhecimento prévio de outros domínios como a cibersegurança da Internet para que o guia proposto pela SAE J3061 seja mais bem conduzido e aplicado.

METODOLOGIA: REVISÃO SISTEMÁTICA DA LITERATURA

A revisão sistemática de literatura (RSL) seguiu o guia proposto por Kitchenham *et al.* (2009) e foi norteada pela seguinte questão principal: [QP] Quais abordagens e aplicações têm sido discutidas nas pesquisas que investigam o uso de ontologias para avaliação de cibersegurança?

Justifica-se a questão principal, considerando a necessidade de aprimorar os sistemas de segurança da informação, o que não é tema novo, mas que, cada vez mais, ganha importância e complexidade. Nesse sentido, pressupomos que o uso de ontologias pode trazer significativos avanços para esse campo do conhecimento aplicado. Sistemas de detecção de intrusão são utilizados desde a década de 1980 e métodos como *data mining*, análise de transição de estados, *clustering*, classificação e *neuro-fuzzy* foram utilizados para reduzir falsos alertas e aumentar a confiabilidade em sistemas de segurança na Internet (ABDOLI; MEIBODY; BAZOUBANDI, 2010). Raskin *et al.* (2001) inauguram um novo campo na segurança da informação com o uso da ontologia.

[2] A Linguagem de Ontologia da Web (OWL) do W3C é uma linguagem da Web Semântica projetada para representar um conhecimento rico e complexo sobre coisas, grupos de coisas e relações entre as coisas.

Os autores defendem que a ontologia é extremamente promissora como ferramenta de classificação para eventos ilimitados (ABDOLI; MEIBODY; BAZOUBANDI, 2010; MOZZAQUATRO *et al*., 2018), afirmando que o conhecimento sobre questões de cibersegurança e medidas de prevenção, integrado a uma ontologia abrangente e acessível às ferramentas de monitoramento, pode melhorar a detecção automática de ameaças à rede IoT e ajudar na implementação dinâmica de serviços adequados de proteção.

Para auxiliar a questão principal de pesquisa, foram criadas três questões específicas, para as quais serão buscadas respostas na literatura acadêmica: [QE1]: Quais as taxonomias que organizam as bases de conhecimento de ataques e vulnerabilidades no contexto da cibersegurança? [QE2]: Quais as estratégias de avaliação em cibersegurança suportadas por ontologias de ataques e vulnerabilidades? [QE3]: Quais as métricas de avaliação em cibersegurança em IoT e CPS?

As questões específicas propostas justificam-se em razão da necessidade de estabelecimento de etapas para responder à questão principal e de especificação dos elementos aplicados a serem analisados na revisão sistemática de literatura. Ao apresentarmos respostas às perguntas específicas, serão discutidos alguns elementos que nos conduzem às respostas à questão principal.

PROTOCOLO DE PESQUISA

O protocolo de pesquisa adotado foi o de busca de artigos em anais de conferências e em revistas científicas, publicados entre 2001 e 2020. O ano de 2001 foi escolhido como período inicial da pesquisa, pois marca o início da utilização de ontologias na solução de problemas de cibersegurança, ataques e vulnerabilidades em sistemas informativos (RASKIN *et al.*, 2001).

As bases de dados escolhidas foram IEEE[3], ACM[4], Elsevier[5] e o portal de periódicos da CAPES[6]. Essas bases foram selecionadas em virtude de serem conhecidas por incluir estudos empíricos ou literatura de pesquisas nas áreas relacionadas à cibersegurança e às ontologias aplicadas à segurança da informação.

Para a pesquisa manual nas bases de dados selecionadas, foram consideradas as seguintes palavras-chave: *"cybersecurity ontology", "cybersecurity assessment", "automotive cybersecurity", "IoT cybersecurity ontology", "CPS Cybersecurity ontology"*. Incluímos também a utilização de *frameworks*, pois esses guias, em sua essência, trazem taxonomias e glossários que harmonizam conceitos em cibersegurança: *"Cybersecurity assessment framework", "Taxonomy of Cyber Attacks", Taxonomy of Vulnerabilities"*. Adicionalmente, foram utilizadas combinações de palavras por meio de conectores lógicos, que formaram a seguinte *string* de busca: [*cybersecurity ontology* AND *cybersecurity assessment framework*], [*cybersecurity ontology* AND (IOT OR CPS OR *automotive*) AND (*assessment OR framework*)].

Além dos procedimentos acima, optou-se por incluir, na RSL, as principais normas de avaliação em cibersegurança em CPS automotivos: norma SAE J3061 e o relatório do NHTSA - DOT HS 812 (*Characterization of Potential Security Threats in Modern Automobiles*), que foram integralmente analisadas em relação as taxonomias que elas citam e empregam [7].

CRITÉRIO DE INCLUSÃO E EXCLUSÃO

Seguindo o protocolo de Kitchenham *et al*. (2009), foram selecionados os artigos que passaram por revisão por pares, publicados entre 2001 e 2020, e discutem: uso de ontologias na solução de problemas de avaliação em cibersegurança em Internet, IoT ou CPS; utilização de taxonomias como forma de organizar bases de dados em ataques e vulnerabilidades; *frameworks* de avaliação e detecção em cibersegurança em IoT ou CPS automotivos; e utilização de métricas de avaliação de segurança cibernética.

[3] Disponível em: https://ieeexplore.ieee.org/Xplore/home.jsp. Acesso em 06 de jan. 2020.

[4] Disponível em: https://dl.acm.org/. Acesso em 06 de jan. 2020

[5] Disponível em: https://www.elsevier.com/pt-br. Acesso em 06 de jan. 2020.

[6] Disponível em: http://www.periodicos.capes.gov.br/. Acesso em 06 de jan. 2020.

[7] As referidas normas são adotadas em todo o setor automotivo mundial, incluindo fabricantes norte-americanos, europeus e asiáticos.

Foram excluídos os artigos que se enquadraram nos seguintes critérios: artigos anteriores a 2001; artigos fora do contexto de cibersegurança, ataques e vulnerabilidades; artigos duplicados do mesmo estudo em revistas diferentes; e dissertações de mestrado, editoriais, prefácios, entrevistas, correspondências, discussões, comentários, cartas, materiais derivados de *workshops* e de painéis.

AVALIAÇÃO DE RELEVÂNCIA

Foram definidos critérios de relevância para classificar os artigos selecionados, com peso de 0 a 1, conforme o quadro 1. Os critérios de relevância foram pesados da seguinte forma: (S) = 1 representa que o critério foi totalmente respeitado; (P) = 0,5 representa que o critério foi parcialmente respeitado; e (N) = 0 representa que o critério não foi respeitado ou é desconhecido.

Quadro 1 − Critérios de relevância

Critério de relevância	Critérios de relevância
QA1	O artigo responde ou contribui claramente com o objetivo da pesquisa?
QA2	O artigo apresenta uma ontologia clara em avaliação de cibersegurança?
QA3	O artigo apresenta um método claro de avaliação de cibersegurança?
QA4	O artigo apresenta evidência de utilização prática de Ontologias em processos de avaliação em cibersegurança?

Fonte: Dados da pesquisa.

Os critérios de relevância da QA1 à QA4 foram avaliados conforme descrição a seguir:

QA1: S (sim), o artigo responde ou contribui claramente para o objetivo da pesquisa; P (parcialmente), o artigo responde de forma implícita; N (não), o artigo não responde de forma clara ou implícita ao objetivo da pesquisa e ele não pode ser facilmente inferido.

QA2: S, os autores confirmaram, no artigo, a existência de uma ontologia clara e declarada; P, os autores pesquisaram e confirmaram uma forma de ontologia ou taxonomia, mesmo que rudimentar; N, os autores pesquisaram e o artigo não inclui alguma referência à ontologia.

QA3: S, o artigo apresenta um guia, *framework* ou método de avalição suportado por alguma ontologia ou taxonomia de avaliação em cibersegurança; P, os autores pesquisaram e confirmaram, de forma indireta, a existência de alguma metodologia de avaliação suportada por ontologia; N, não foi possível identificar, de forma clara ou indireta, a existência de um guia ou método de avaliação.

QA4: S, o artigo apresenta exemplos práticos de avaliação em cibersegurança, com suporte ontológico; P, o artigo apresenta exemplo(s), mesmo que de forma indireta, do uso de ontologia na avaliação em cibersegurança; N, não apresenta exemplos.

PROCESSO DE EXTRAÇÃO

Durante o processo de busca e extração, foram encontrados 785 artigos em conformidade com os critérios adotados. Num segundo estágio, removemos artigos duplicados em razão das diferentes bases de dados. Na terceira fase, eliminamos artigos cujos títulos não tinham relação com o tema proposto e, na quarta fase, removemos artigos cujo resumo não apresentava relação com o objetivo da pesquisa.

Foram recuperados 18 artigos, após a aplicação dos filtros, de acordo com o protocolo estabelecido, e que respondem às QEs. Realizado o processo de recuperação, lemos os artigos selecionados em sua integralidade e aplicamos os critérios de relevância.

CLASSIFICAÇÃO DOS ARTIGOS

Os artigos foram classificados em áreas de interesse que correspondem aos objetivos da pesquisa: TXN_ATQ (Taxonomia de ataques e vulnerabilidades); AVAL_ONTO (Avaliação através de ontologia em cibersegurança); MTR (Métricas de avaliação); e FRM_WK (*Frameworks* de avaliação em cibersegurança). A classificação oferece uma forma de agrupar os artigos conforme as questões auxiliares desta pesquisa:

ARTIGOS SELECIONADOS

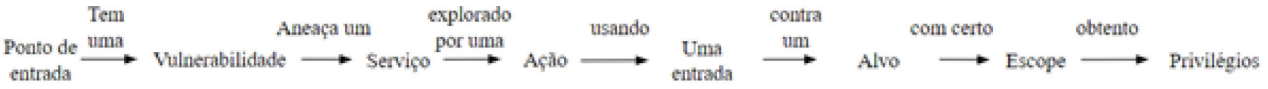
A Tabela 1 a seguir apresenta os artigos selecionados e seus autores, além dos respectivos repositórios.

Tabela 1 − Artigos selecionados

Autor / Ano	Título	Revista / Conferência	Repositório	Classificação
Abdoli, Meibody e Bazoubandi (2010)	An Attacks Ontology for computer and networks attack	*Innovations and Advances in Computer Sciences and Engineering*	Springer	AVAL_ONTO
Ficco (2013)	Security event correlation approach for cloud computing	*International Journal of High Performance Computing and Networking*	Researchgate	AVAL_ONTO
Georgescu e Smeureanu (2017)	*Using Ontologies in Cybersecurity Field*	*Informática Econômica*	Researchgate	AVAL_ONTO
Álvarez e Petrović (2003)	*A new taxonomy of Web attacks suitable for efficient encoding*	*Computer and Security*	Elsevier	TXN_ATQ
Igure e Williams (2008)	*Taxonomies of attacks and vulnerabilities in computer systems*	*Communications Surveys & Tutorials*	IEEE	TXN_ATQ
Hansman e Hunt (2005)	*A taxonomy of network and computer attacks*	*Computer and Security*	Elsevier	TXN_ATQ
Mozzaquatro *et al.* (2018)	*An Ontology-Based Cybersecurity Framework for the Internet of Things*	*Sensors*	MDPI	FRM_WK
Tao *et al.* (2018)	*Multi-layer cloud architectural model and ontology-based security service framework for IoT-based smart homes*	*Future Generation Computer Systems*	MDPI	AVAL_ONTO
Mccarthy, Harnett e Carter. (2014)	*Characterization of potential security threats in modern automobiles: A composite modeling approach.*	-	NHTSA	FRM_WK
Schmittner *et al.* (2016)	*Using SAE J3061 for Automotive Security Requirement Engineering*	*Computer Safety, Reliability, and Security*	Springer	FRM_WK
SAE J3061 (2016)	*Cybersecurity guidebook for cyber-physical automotive systems*	-	SAE	FRM_WK
Balduccini *et al.* (2018)	*Ontology-Based Reasoning about the Trustworthiness of Cyber-Physical Systems*	*Living in the Internet of Things: Cybersecurity of the IoT*	IEEE	AVAL_ONTO
Wu, Zhang e Cao (2017)	*Safety Guard: Runtime Enforcement for Safety-Critical Cyber-Physical Systems: Invited*	*DAC proceedings*	ACM	FRM_WK
Razzaq *et al.* (2014)	*Ontology for attack detection: An intelligent approach to web application security*	*Computer and Security*	Elsevier	MTR
Homer *et al.* (2013)	*Aggregating vulnerability metrics in enterprise networks using attack graphs*	*ARES proceedings*	ACM	MTR
Bergner e Lechner (2017)	*Cybersecurity Ontology for Critical Infrastructures*	*International Conference on Knowledge Engineering and Ontology Development*	SCI	AVAL_ONTO
Fenz e Ekelhart (2006)	*Security Ontology: Simulating Threats to Corporate Assets*	*Book Session: Information Systems Security*	Springer	AVAL_ONTO
Griffor (2017)	*Framework for Cyber-Physical Systems*	-	NIST	FRM_WK

Fonte: Dados da pesquisa.

Figura 2 − Taxonomia de ataques na web



Fonte: Adaptado de Álvarez *et al.* (2003).

ANÁLISE E DISCUSSÃO DOS RESULTADOS

Com os artigos selecionados, foi possível responder às questões de pesquisa deste trabalho, conforme apresentado a seguir.

[QE1]: Quais taxonomias organizam as bases de conhecimento de ataques e vulnerabilidades no contexto da cibersegurança?

Os ataques contra ativos informacionais estão se tornando cada vez mais sofisticados, distribuídos e com rápida difusão. Portanto, é necessário classificá-los por meio de taxonomias. Esse tipo de classificação pode ser usado na execução sistemática da avaliação da cibersegurança de um sistema.

Álvarez e Petrović (2003) propuseram uma taxonomia de ataques na web adequada a uma codificação eficiente, usando como referência o ponto de entrada do sistema, onde existe uma vulnerabilidade que ameaça um serviço, contra um alvo de escopo determinado, obtendo, assim, certo privilégio como permissão administrativa.

A taxonomia dos autores definiu um esquema semântico de codificação dos ataques na web, removendo redundâncias na descrição dos ataques, o que gerou economia de tempo e memória no processamento. A codificação e a economia no esforço computacional permitiram sua utilização em sistemas de detecção de intrusão, como *firewalls*.

Os autores evidenciam que a aplicação de um IDS (*Intrusion Detection System*) pode funcionar melhor com a utilização da taxonomia, pois seu emprego permite que sejam gerados menos falsos alertas que um *firewall* tradicional. Conforme destacam os autores, a eficácia no bloqueio de ataques e a decisão sobre sua gravidade são cruciais para uma resposta eficaz. A taxonomia ajuda nessa tarefa ao prover um grupo exaustivo de categorias exclusivas por meio das quais os ataques podem ser classificados sem ambiguidade, através de métodos que empregam o esquema de classificação.

Hansman e Hunt (2005) utilizaram a base de dados do projeto CVE[8] (*Common Vulnerabilities and Exposures*) como parte da sua taxonomia de ataque. *Corpus* como o CVE são extremamente úteis pela sua ampla base de conhecimento sobre vulnerabilidades em diversos sistemas operacionais. O projeto CVE, originalmente proposto por Baker *et al.* (1999), teve apoio do *U.S. Department of Homeland*. A comunidade de cibersegurança endossou a importância do CVE via produtos compatíveis (CVE-*compatible*) e, em 2011, o DISA (*U.S. Defense Information Systems Agency*) determinou que fabricantes e distribuidores apresentassem identificadores CVE em produtos utilizados por aquela agência.

Assim como o CVE, o NVD[9] (*U.S. National Vulnerability Database*) é um banco de dados abrangente sobre vulnerabilidades em cibersegurança, que integra todos os recursos de vulnerabilidade do governo dos EUA disponíveis publicamente e fornece referências à indústria. As informações do NVD podem ser acessadas através de web semântica e seus dados permitem a automação do gerenciamento de vulnerabilidades, medição de segurança e conformidade. O banco de dados da NVD inclui referências a listas de verificação de segurança, falhas de software relacionadas à segurança, configurações incorretas, nomes de produtos e métricas de impacto.

[8] CVE (Common Vulnerabilities Exposures) está disponível em http://cve.mitre.org. Acesso em 19 janeiro de 2019.

[9] NVD (US National Vulnerability Database) está disponível em https://nvd.nist.gov. Acesso em 06 março de 2019.

O CVSS (*Common Vulnerability Scoring System*) disponível no NVD fornece uma estrutura aberta de comunicação das características e impactos das vulnerabilidades em tecnologia da informação (TI). Seu modelo é quantitativo e permite aos usuários uma confiabilidade no processo de avaliação. Assim, o CVSS é bem adequado como um sistema de medição padronizada para indústrias, organizações e governos que necessitam de pontuações consistentes de impacto de vulnerabilidade.

Em resumo, as taxonomias de ataques nos dão uma visão de padrões de ataques. Podemos dizer que o padrão de ataque é uma sequência de passos do ataque contra uma fraqueza a ser explorada em um software e ajuda a identificar e qualificar o risco de um determinado ataque. Os padrões de ataques tornaram-se mais viáveis em termos computacionais após a criação e definição formal de taxonomias como a *Common Attack Pattern Enumeration and Classification* (CAPEC) e CVE (BARNUM, 2012). A Tabela 2 apresenta um resumo das principais bases de dados que permitem aos desenvolvedores se guiar e compartilhar informações sobre ataques e vulnerabilidades. As bases de dados permitem ao desenvolvedor eliminar ambiguidades e aumentar a precisão, bem como automatizar, integrar e correlacionar dados e processos, permitindo um desenvolvimento rápido de contramedidas.

Tabela 2 – Principais bases de dados em cibersegurança

Recurso	Descrição	Propósito	Site
CAPEC	*Common Attack Pattern Enumeration and Classification*	Fornece um catálogo publicamente disponível de padrões de ataque, juntamente com um esquema abrangente e taxonomia de classificação	https://capec.mitre.org/
NVD	*National Vulnerability Database*	O NVD é o repositório do governo dos EUA de dados de gerenciamento de vulnerabilidade baseados em padrões representados usando o SCAP (*Security Content Automation Protocol*)	https://nvd.nist.gov/
JVN	*JAPAN Vulnerability Notes*	Fornece informações de vulnerabilidade em japonês e é descrito de acordo com seu próprio esquema em RDF	https://jvn.jp/en/
CVE	*Common Vulnerabilities and Exposures*	Dicionário de descrições padronizadas para vulnerabilidades e exposições	http://cve.mitre.org
CWE	*Common Weakness Enumeration*	Lista de fraquezas comuns de segurança de software desenvolvidas pela comunidade. Ela serve como uma linguagem comum, uma ferramenta de medição para ferramentas de segurança de software e como uma linha de base para esforços de identificação, mitigação e prevenção de fraquezas.	https://cwe.mitre.org/

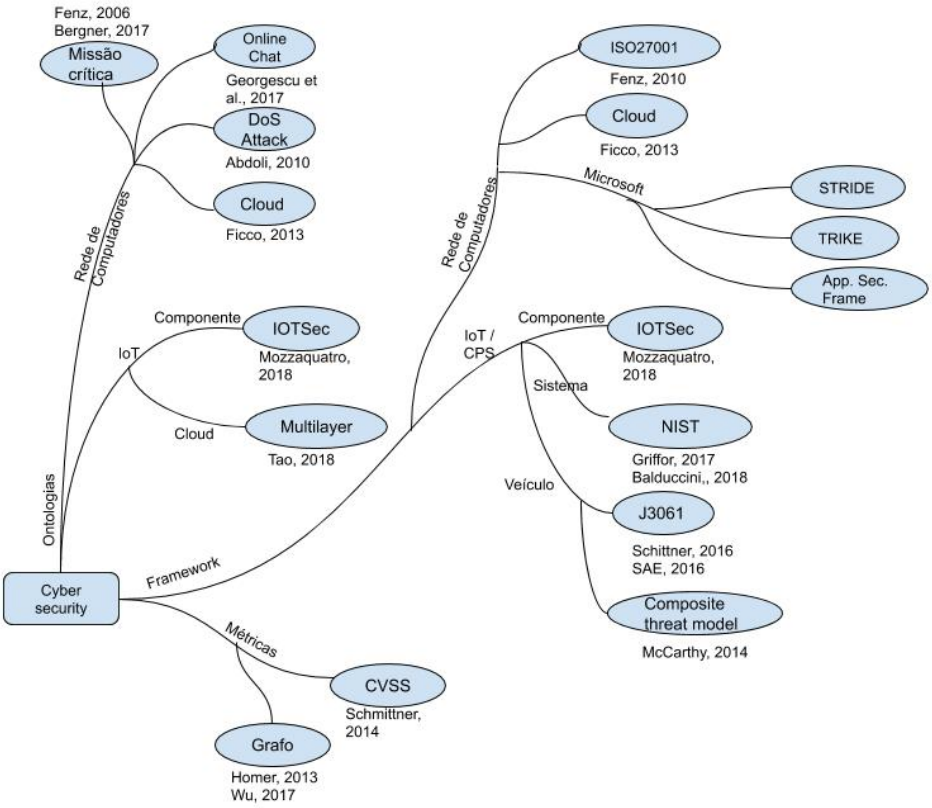
Fonte: Elaborada pelo autor.

[QE2]: Quais são as estratégias de avaliação em cibersegurança suportadas por ontologias de ataques e vulnerabilidades?

Avaliação de risco é um componente da gestão de gestão de segurança da informação voltado à identificação de ameaças e vulnerabilidades, potenciais impactos decorrentes da perda de confidencialidade, integridade e/ou disponibilidade de ativos de informação.

Nafigura 3, é apresentado um resumo das principais ontologias e métodos de avaliação encontrados durante a revisão sistemática. O critério que utilizamos para a construção da árvore foi baseado na classificação de artigos empreendida por Petersen *et al.* (2008). Os autores recomendam a busca de facetas coincidentes nos artigos e elaboração de um mapa esquemático para agrupá-los em grupos e subgrupos. O resultado visto é apresentado na figura 3, com os grupos de ontologias, *frameworks* e métricas, além dos subgrupos de rede de computadores, IoT e CPS automotivos.

Figura 3 − Principais ontologias e *frameworks* de avaliação em cibersegurança



Fonte: Elaborada pelo autor.

A revisão abordou dois grandes construtos: ontologias e *frameworks* de cibersegurança. Dentro desses construtos, o mapa da figura 3 fornece os domínios de interesse da revisão sistemática: Rede de computadores e IoT/CPS. Na sequência, descrevemos as pesquisas recuperadas dentro de cada domínio.

Abdoli, Meibody e Bazoubandi (2010) desenharam uma ontologia para ataques em computadores e redes de computadores. Os autores estudaram diferentes números de conexões e logs que causaram ataques do tipo DoS (*Denied of Service*). A utilização do *Protégé* e SPARQL suportou análises e raciocínios de sequências de logs extensas. A importância desse estudo é que ele não somente comprovou a efetividade da análise holística que a ontologia proporciona, mas também apresentou uma forma efetiva de integração entre conhecimento sobre tipos de ataques e estudos de casos reais. Nesse tipo de situação, o desafio da equipe de segurança da informação é analisar sequências de informações que envolvem grande quantidade de parâmetros e dados que podem ou não indicar ataques.

Ficco (2013) utilizou a mesma estratégia de análise para *cloud computing* ao investigar passos de ataques mediante correlação de eventos de segurança. O processo de detecção de intrusão empregou uma abordagem híbrida, capaz de analisar eventos por meio de ontologia, para detectar sintomas de intrusão em computação distribuída. Uma *query* foi usada para analisar uma sequência de requisições a partir de uma base de conhecimento sobre ameaças, com a finalidade de decidir quando um comportamento particular representava uma ameaça potencial.

Geogescu e Smeureanu (2017) utilizaram a web semântica para extração de textos *on-line* em linguagem natural para detectar atividades de *black hat hackers*.

Os autores encontraram correlação entre atividades dos hackers e fontes de informação como fóruns e chats privados, resultando em uma forma de extrair informações para avaliação das ameaças que vão além dos bancos de dados da CVE (*Common Vulnerabilities Exposures*) e também do conhecimento adquirido pelos engenheiros de cibersegurança. Na abordagem dos autores, as fontes de informações podem ser fóruns, blogs, websites e chats privados. As informações, extraídas por meio de scrapers, foram carregadas em uma ontologia e, em seguida, geradas estatísticas de possíveis atividades atribuídas aos hackers. No sistema desenvolvido pelos autores, raciocinadores são empregados na emissão de notificações, aumentando, assim, a eficiência na análise de uma massa de dados.

Mozzaquatro *et al.* (2018) propuseram um *framework* de avaliação em cibersegurança de componentes básicos utilizados na IoT e seus processos por meio da ontologia IoTSec[10]. Essa ontologia foi desenhada para reunir conhecimento sobre alertas e possíveis ameaças e ataques, prover a capacidade de raciocinar e descobrir dados implícitos em uma informação sobre problemas de cibersegurança.

No exemplo utilizado durante o trabalho, os autores mostraram como o ambiente IoT é frequentemente suscetível às ameaças em uma rede Wi-Fi em razão de pontos de acesso mal configurados, interceptação de dados e negação de serviço. A figura 4 apresenta o resultado da *query* que emprega a ontologia IoTSec. O resultado da consulta mostra as vulnerabilidades em ativos da rede, as criptografias disponíveis e o *status* atual: reprovado ou seguro.

[10] IoTSec disponível em http://iotsec.brunomozza.com/. Acesso em 6 mar. 2019.

Figura 4 – Exemplo de *query* proposta pelo *framework* de Mozzaquatro *et al.* (2018)

```
SELECT ?ASSET ?VULN ?THREAT ?SECPROP ?SECMEC_1 ?FEATURE_1
WHERE {
  ?VULN iotsec:isVulnerabilityOf ?ASSET .
  ?VULN iotsec:isThreatensBy ?THREAT .
  ?THREAT iotsec:affects ?SECPROP .
  ?SECMEC_1 iotsec:isSecurityMechanismOf ?THREAT .
  ?SECMEC_1 iotsec:hasFeature ?FEATURE_1 .
  ?SECMEC_1 rdfs:label ?SMLabel .
  FILTER regex (?SMLabel, 'WEP')
}
```

ASSET	VULNERABILITY	THREAT	SECURITYPROPERTY	SECMEC_1	FEATURE_1	SM_2	FEAT_2
WiFi	UnauthorizedAccess	Eavesdropping	Authentication	WEP	Deprecated	WPA1	Deprecated
WiFi	UnauthorizedAccess	Eavesdropping	Authentication	WEP	Deprecated	WPA2	Secured

Fonte: Mozzaquatro *et al.* (2018).

Tao *et al*. (2018) propuseram uma ontologia para cibersegurança em IoT, fundamentada em um modelo de arquitetura em nuvem multicamadas, para permitir interações entre os dispositivos IoT de *smart homes*, que geram uma grande quantidade de dados. A importância da ontologia criada pelos autores decorre do fato de a heterogeneidade de dispositivos, serviços, protocolos de comunicação, padrões e formatos de dados envolvidos nas *smart homes*, oriundos de diferentes fornecedores, afetar negativamente a utilização e proliferação da IoT. A ontologia desenvolvida pelos autores suporta a representação dos dados, conhecimentos, serviços de segurança entre o provedor de serviço e os usuários. A ontologia define um grupo comum de vocabulário, um objetivo de segurança, como integridade através de assinatura digital, confidencialidade por encriptação e um *token* de segurança. Por meio da ontologia proposta, fabricantes de dispositivos seriam capazes de definir políticas de segurança, indicando a habilidade de interações e interoperações.

Mccarthy, Harnett e Carter (2014) caracterizaram o primeiro modelo de potenciais ataques em veículos automotores. Com o objetivo de aprimorar as melhores práticas de segurança cibernética na indústria automotiva, os autores reuniram informações em uma base de conhecimento coletivo sobre segurança cibernética automotiva, visando a ajudar a descrever os ambientes de risco e ameaças, além de dar suporte a tarefas de acompanhamento usadas para estabelecer diretrizes de segurança durante o desenvolvimento de automóveis.

Os autores desenvolveram ferramentas de avaliação e requisitos de mínima performance para cibersegurança automotiva, baseando-se nos modelos da Microsoft *Composite Threat Model* STRIDE, TRIKE e *Application Security Frame* (MCCARTHY; HARNETT; CARTER, 2014). O *framework* adotado pelos autores foi dividido em duas partes: a primeira identifica as aplicações e sistemas críticos e a segunda determina e analisa as ameaças por intermédio de uma matriz de potenciais ataques, nível de sofisticação, dificuldade de implementação e probabilidade de ocorrência.

Schmittner *et al.* (2016) mostraram a utilização do TARA (Threat Analysis and Risk Assessment), que suporta avaliação de risco a partir de um cenário de ataque para ajudar organizações a identificar e avaliar ameaças envolvidas no design em cibersegurança em CPS automotivos, desde a fase de conceito, produção, operação, serviço e de comissionamento. Nota-se que a avaliação de risco seguida pelos autores é uma adaptação do projeto HEAVENS proposto por Schmittner *et al.* (2014) e também recomendado pela norma J3061.

Na pesquisa de Schmittner *et al.* (2016), a avaliação de risco recebeu pontuações conforme a: (1) capacidade de execução do ataque; (2) disponibilidade de informação do sistema alvo; (3) acessibilidade ao alvo; e (4) tecnologia necessária para comprometer remotamente um sistema do automóvel (Tabela 3).

Tabela 3 − Exemplo de avaliação de risco em ativos automotivos

Attack Scenario	Threat	Effect	Attack Probability	Severity	Risks
Asset: Software/Applications					
Exploit Known vulnerabilities in OS or applications remotely	Install rootkit, Trojan	Take control of system CPS operations, change parameters, and access data	9 (2+1+3+3)	4	High
Exploit Known vulnerabilities in OS or application remotely	Delete software component	Reduce functionality of CPS	9 (2+1+3+3)	2	Medium

Fonte: Schmittner *et al.* (2016)

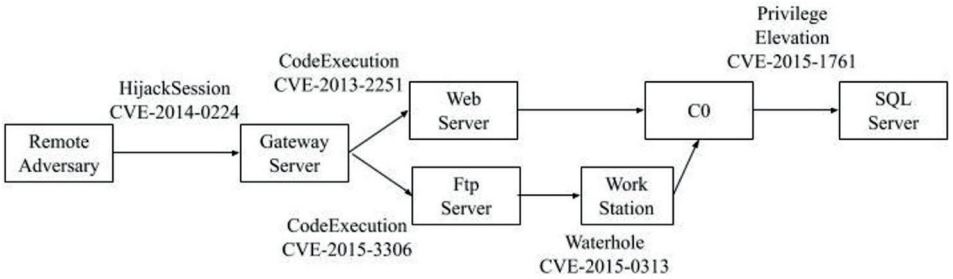
O NIST (U.S. National Institute of Standards and Technology) hospedou um grupo de trabalho público sobre sistemas físicos cibernéticos (CPS) com o objetivo de identificar insumos envolvidos em CPS para definir um framework de referência que contivesse definições comuns e facilitasse a interoperabilidade entre tais sistemas. Balduccini *et al.* (2018), tendo como referência o trabalho desse grupo, descreveram uma avaliação de fidedignidade através de uma ontologia voltada a safety, confiabilidade, security, resiliência e privacidade. Merecem destaque, no referido trabalho, a utilização da ontologia e a avaliação de confiança em um sistema de LKAS (lane keeping assistant), ou seja, um sistema que tem a finalidade de manter um automóvel dentro da sua pista, utilizando duas câmeras de vídeo. Caso o CPS perceba que o automóvel abandonou sua faixa de rolamento, o sistema assume o volante na tentativa de corrigir a rota do veículo. Esse sistema utiliza câmeras e radares para atuar. Os autores fizeram uma avaliação do sistema por meio de conexões com algumas bases de dados de ameaças e ataques, como proposto por Hansman e Hunt (2005). Ainda, Balduccini *et al.* (2018) mostraram, em um caso de uso, como hackear o sistema LKAS e operá-lo externamente, invertendo as imagens gravadas pelas câmeras, o que ocasionou perda de imagens, consequentemente falha em segurança (safety), e a contramedida, utilizando uma ontologia de dois níveis.

[QE3]: Quais as principais métricas de avaliação em cibersegurança em IoT e CPS?

Durante a análise da QE1, algumas métricas de avaliação já foram apontadas, como aquelas apresentadas no projeto HEAVENS, de Schmittner *et al.* (2014), no CVSS do NVD e nos modelos Microsoft STRIDE. Além dessas, métricas que empregam grafos também são importantes ferramentas para avaliação de ataques complexos, nos quais hackers precisam seguir vários passos até conseguirem um ataque bem-sucedido.

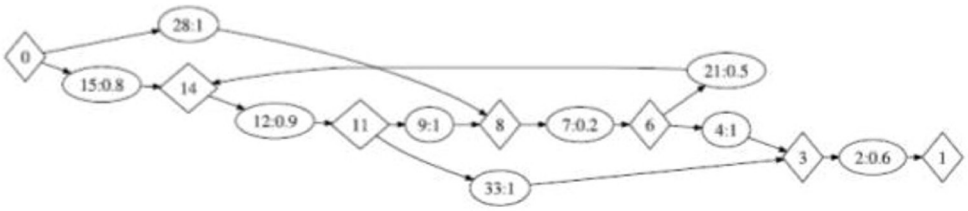
Wu, Zhang e Cao (2017) utilizaram grafos para dar suporte a administradores de TI no combate aos ataques cujos alvos são vários servidores. A combinação de máquinas e serviços em redes corporativas é cada vez mais complexa e, nesse contexto, torna-se uma tarefa difícil para administradores avaliarem a segurança geral da rede. Para manter a segurança e a disponibilidade da infraestrutura, um vocabulário e soluções automatizadas comuns são uma importante ferramenta para troca de conhecimento de segurança e análise de possíveis ataques. Gráficos de ataque ajudam a ilustrar os caminhos de ataques em vários estágios, que são potencialmente complexos. Além disso, um grafo pode ajudar a quantificar uma sequência de requisições a uma rede distribuída, o que torna mais objetiva a análise de possíveis ameaças a um sistema (figura 5).

Figura 5 − Passos de ataque representados por meio do grafo



Fonte: Wu, Zhang e Cao (2017)

Figura 6 - Grafo de ataque e as métricas geradas a cada passo utilizando a CVSS



0: Attacker Located internet
1: execCode(dbServer, root)
2: remote exploit of CVE-2009-2446
3: netAccess(dbServer,tcp,3306)
4: multi-hop access
6: execCode(webServer,apache)
7: remote exploit of CVE-2006-3747]
8: net Access(webServer, tcp,80)
9: multi-hop access
11: execCode(workStation, user Account)
12: remote exploit of CVE-2009-1918
14: access Malicious Input (WorkStation, user, IE)
15: victim browse a malicious website
21: victim browse a compromised website
28: direct network access
33: multi-hop access

Fonte: Homer *et al.* (2013).

Homer *et al.* (2013) agregaram métricas de avaliação de risco a redes corporativas para os gráficos de ataque, com vistas a trazer informações objetivas, que levem a responder a questões como, por exemplo: se uma determinada modificação for feita na rede corporativa, ela se torna mais ou menos vulnerável? Os autores basearam-se em métricas da CVSS (Commom Vulnerability Scoring Systems), combinando-as com os possíveis passos de um provável ataque, gerando métricas de risco de segurança por intermédio de pontos cumulativos de cada passo do ataque (figura 6).

No exemplo, o privilégio inicial do atacante é 0 (Internet) e, para ganhar o privilégio 14 (workstantion), é necessário lançar o exploit 15 (victim browse a malicious website). A probabilidade de chegar ao privilégio 14 é dada pela CVSS como 0,8. O próximo passo do ataque é ganhar os privilégios 11, 8, 6 e 3, por meio de outros mecanismos de exploit, até o atacante chegar ao privilégio 1 (root). A métrica gerada é a somatória dos passos, que parte de 0 até 1, e seus relativos pesos nos dão a dimensão do risco. Essa métrica pode nortear ações de administradores através de ações para mitigar ou eliminar a vulnerabilidade

CONCLUSÕES

O uso de ontologias em cibersegurança é defendido por vários autores tendo em vista a rapidez e a forma holística de tratar muitos parâmetros na avaliação dos riscos envolvidos. A representação formal pode suportar desenvolvedores e também estabelecer um conhecimento formal e compartilhado sobre ataques e vulnerabilidades.

Em todos os trabalhos que foram objeto de análise na RSL realizada, denota-se a clara necessidade de organização ontológica para facilitar e unificar o entendimento dos stakeholders envolvidos na tarefa de avaliar riscos e implementar soluções para cibersegurança, não importando se direcionadas a uma rede de computadores, a uma IoT ou a um CPS. Respondendo de maneira ampla à questão de pesquisa colocada, os artigos que abordam a avaliação em cibersegurança podem ser divididos em dois grupos principais. No primeiro, os autores utilizam ontologias na etapa de desenvolvimento de sistemas para avaliação dos requisitos de segurança (MCCARTHY; HARNETT; CARTER, 2014; SCHMITTNER *et al.*, 2016; MOZZAQUATRO *et al.*, 2018; TAO *et al.*, 2018). No segundo, estão as pesquisas referentes aos sistemas em operação. Nesses casos, seja na Internet seja em IoT, os autores utilizam ontologias com o suporte de raciocinadores para identificar padrões e prever ataques (HANSMAN; HUNT, 2005; GEORGESCU; SMEUREANU, 2017; BALDUCCINI *et al.*, 2018).

Tanto no desenvolvimento quanto na operação, os domínios influenciaram a construção das ontologias (figura 3). No caso de um IoT ou um CPS trabalhando em multicamadas, por exemplo, a ontologia de Tao *et al.* (2018) e o framework de sistema do NIST (GRIFFOR *et al.*, 2017) mostraram-se mais adequados à solução, ao passo que o mesmo CPS/IoT, no domínio do componente, poderia ser mais adequado ao IoTSec, de Mozzaquatro, Jardim-Goncalves, Agostinho (2015).

Seja no desenvolvimento seja na operação, as avaliações de cibersegurança utilizam métricas reconhecidas pelo mercado, como o CVSS e o CVE . Essas métricas estão disponíveis em bases de conhecimento sobre ameaças e vulnerabilidades do NVD (National Vulnerability Database) e CWE (Common Weakness Enumeration), e são utilizadas pelos autores como referência para lidar com vulnerabilidades (HANSMAN; HUNT, 2005; GEORGESCU; SMEUREANU, 2017; HOMER *et al.*, 2013; BALDUCCINI *et al.*, 2018).

Os trabalhos em cibersegurança na Internet pavimentaram os estudos realizados posteriormente em IoT, CPS e, consequentemente, no mundo automotivo. A adoção rápida do NHTSA como padrão de análise em cibersegurança e a elaboração de procedimentos como o HEAVENS da norma J3061 mostram a importância do tema no setor automotivo.

Apesar de a aplicação da IoT no domínio automotivo ser relativamente recente, os conhecimentos já consolidados sobre cibersegurança no ambiente da Internet e as pesquisas já realizadas sobre ontologias de avaliação em cibersegurança são fundamentais para o avanço na sua utilização em CPS. Quanto a isso, o framework da norma J3061, com as métricas de CVSS, as ontologias do IoTSec de Mozzaquatro *et al.* (2018) e a ontologia em multicamadas de Tao *et al.* (2018) mostram-se adequado a esse tipo de aplicação.

REFERÊNCIAS

ABDOLI, F.; MEIBODY, N.; BAZOUBANDI, R. An Attacks Ontology for computer and networks attack. *In:* SOBH, T. (ed.). Innovations and Advances in Computer Sciences and Engineering, 2008. *Proceedings* […]. Dordrecht: Springer Netherlands, 2010. DOI https://doi.org/10.1007/978-90-481-3658-2_83. Disponível em: https://link.springer.com/book/10.1007/978-90-481-3658-2#toc. Acesso em: mar. 2021.

ABDULKHALEQ, A. *et al.* Using STPA in Compliance with ISO 26262 for Developing a Safe Architecture for Fully Automated Vehicles. *arXiv:1703.03657*, p. 11-24, 10 Mar. 2017. Disponível em: https://arxiv.org/abs/1703.03657. Acesso em: jun. 2021.

ALAM, S.; CHOWDHURY, M. M.; NOLL, J. Interoperability of security-enabled internet of things. *Wireless Personal Communications*, v. 61, n. 3, p. 567–586, 2011. DOI https://doi.org/10.1007/s11277-011-0384-6. Disponível em: https://link.springer.com/article/10.1007/s11277-011-0384-6. Acesso em: jan. 2021.

ALI, N.; HONG, J. E. Failure Detection and Prevention for Cyber-Physical Systems Using Ontology-Based Knowledge Base. *Computers,* v. 7, n. 4, p. 68-84, Dec. 2018. DOI https://doi.org/10.3390/computers7040068. Disponível em: https://www.mdpi.com/2073-431X/7/4/68. Acesso em: maio 2021.

ALMEIDA, M. B. Um modelo baseado em ontologias para representação da memória organizacional. *Perspectivas em Ciência da Informação*, Belo Horizonte, v. 11, n. 3, p. 449–449, dez. 2006. Disponível em: http://portaldeperiodicos.eci.ufmg.br/index.php/pci/article/view/38. Acesso em: mar. 2021.

ALMEIDA, M. B. Revisiting ontologies: A necessary clarification. *Journal of the American Society for Information Science and Technology*, v. 64, n. 8, p. 1682–1693, 2013. DOI https://doi.org/10.1002/asi.22861. Disponível em: https://onlinelibrary.wiley.com/doi/10.1002/asi.22861. Acesso em: fev. 2021.

ÁLVAREZ, G.; PETROVIĆ, S. A new taxonomy of Web attacks suitable for efficient encoding. *Computers & Security*, v. 22, n. 5, p. 435–449, Jul. 2003. DOI https://doi.org/10.1016/S0167-4048(03)00512-1. Disponível em: https://www.sciencedirect.com/science/article/pii/S0167404803005121. Acesso em: abr. 2021.

BAKER, D. W. *et al.* The Development of a Common Enumeration of Vulnerabilities and Exposures. *In:* INTERNATIONAL WORKSHOP ON RECENT ADVANCES IN INTRUSION DETECTION, 2., 1999. *Proceedings* […]. Virginia: MITRE, 1999. Diponível em: https://cve.mitre.org/docs/docs-2001/Development_of_CVE.html. Acesso em: fev. 2021.

BALDUCCINI, M. *et al.* Ontology-Based Reasoning about the Trustworthiness of Cyber-Physical Systems. *In:* LIVING IN THE INTERNET OF THINGS: CYBERSECURITY OF THE IOT, London, 28-29 Mar. 2018. *Proceedings* […]. London: IET Digital Library, 2018. DOI 10.1049/cp.2018.0012. Disponível em: https://digital-library.theiet.org/content/conferences/10.1049/cp.2018.0012. Acesso em: abr. 2021.

BARNUM, S. Standardizing cyber threat intelligence information with the Structured Threat Information eXpression (STIX). *Mitre Corporation*, v. 11, p. 1–22, Jan. 2012. Disponível em: https://www.mitre.org/publications/technical-papers/standardizing-cyber-threat-intelligence-information-with-the. Acesso em: maio 2021.

BERGNER, S.; LECHNER, U. Cybersecurity Ontology for Critical Infrastructures. *In:* INTERNATIONAL JOINT CONFERENCE ON KNOWLEDGE DISCOVERY, KNOWLEDGE ENGINEERING AND KNOWLEDGE MANAGEMENT (KEOD), 9., 2017, Portugal. *Proceedings* […]. Portugal: IC3K, 2017. DOI 10.5220/0006510400800085.

EKELHART, A.; FENZ, S.; NEUBAUER, T. Aurum: A framework for information security risk management. *In:* HAWAII INTERNATIONAL CONFERENCE ON SYSTEM SCIENCES, 42., 2009, Waikoloa, USA. *Proceedings* [...]. USA: IEEE, 2009. DOI 10.1109/HICSS.2009.82. Disponível em: https://ieeexplore.ieee.org/document/4755409. Acesso em: jan. 2021.

FICCO, M. Security event correlation approach for cloud computing. *International Journal of High Performance Computing and Networking*, v. 7, n. 3, p. 173–185, Sep. 2013. Disponível em: https://doi.org/10.1504/IJHPCN.2013.056525. Acesso em: fev. 2021.

GEORGESCU, T.; SMEUREANU, I. Using Ontologies in Cybersecurity Field. *Informatică economică*, Romania, v. 21, n. 3, p. 5–15, 2017. DOI 10.12948/issn14531305/21.3.2017.01. Disponível em: https://revistaie.ase.ro/83.html. Acesso em: mar. 2021.

GRIFFOR, E. (ed.). *Framework for cyber-physical systems:* volume 1, overview. Gaithersburg, MD: National Institute of Standards and Technology, Jun. 2017. Disponível em: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1500-201.pdf. Acesso em: 2 ago. 2018.

GRUBER, T. R. A translation approach to portable ontology specifications. *Knowledge Acquisition*, v. 5, n. 2, p. 199–220, Jun. 1993. DOI https://doi.org/10.1006/knac.1993.1008. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S1042814383710083. Acesso em: maio 2021.

HAMMONS, R. L.; KOVAC, R. J. (ed.). *Fundamentals of internet of things for non-engineers*. Boca Raton: Auerbach Publications, 2019. (Technology for non- engineers).

HANNON, E. *et al*. What's driving the connected car. *McKinsey&Company*, 1 Sep. 2014. Disponível em: https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/whats-driving-the-connected-car. Acesso em: 27 ago. 2018.

HANSMAN, S.; HUNT, R. A taxonomy of network and computer attacks. *Computers & Security,* v. 24, n. 1, p. 31–43, Feb. 2005. DOI https://doi.org/10.1016/j.cose.2004.06.011. Disponível em: https://www.sciencedirect.com/science/article/pii/S0167404804001804. Acesso em: maio 2021.

HERZOG, A.; SHAHMEHRI, N.; DUMA, C. An ontology of information security. *International Journal of Information Security and Privacy (IJISP)*, v. 1, n. 4, p. 1–23, 2007. Disponível em: https://www.igi-global.com/article/ontology-information-security/2468. Acesso em: fev. 2021.

HOMER, J. *et al.* Aggregating vulnerability metrics in enterprise networks using attack graphs. *Journal of Computer Security*, v. 21, n. 4, p. 561–597, Sep. 2013. DOI 10.3233/JCS-130475. Disponível em: https://content.iospress.com/articles/journal-of-computer-security/jcs475. Acesso em: jan. 2021.

IBARRA-ESQUER, J. *et al.* Tracking the evolution of the Internet of things concept across different application domains. *Sensors*, v. 17, n. 6, p. 1379-1402, Jun. 2017. DOI https://doi.org/10.3390/s17061379. Disponível em: https://www.mdpi.com/1424-8220/17/6/1379/htm. Acesso em: jun. 2021.

IGURE, V. M.; WILLIAMS, R. D. Taxonomies of attacks and vulnerabilities in computer systems. IEEE *Communications Surveys & Tutorials*, United States, v. 10, n. 1, p. 6-19, 2008. DOI 10.1109/COMST.2008.4483667. Disponível em: https://ieeexplore.ieee.org/document/4483667. Acesso em: fev. 2021.

KHAZAI, B. *et al*. VuWiki: An Ontology-Based Semantic Wiki for Vulnerability Assessments. *International Journal of Disaster Risk Science*, v. 5, n. 1, p. 55–73, Mar. 2014. DOI https://doi.org/10.1007/s13753-014-0010-9. Disponível em: https://link.springer.com/article/10.1007/s13753-014-0010-9. Acesso em: abr. 2021.

KITCHENHAM, B. *et al.* Systematic literature reviews in software engineering: a systematic literature review. *Information and software technology*, v. 51, n. 1, p. 7–15, Jan. 2009. Disponível em: https://doi.org/10.1016/j.infsof.2008.09.009. Acesso em: maio 2021.

MACHER, G. *et al*. A review of threat analysis and risk assessment methods in the automotive context. *In:* INTERNATIONAL CONFERENCE ON COMPUTER SAFETY, RELIABILITY, AND SECURITY, Sep. 2016, Trondheim, Norway. *Proceedings* [...]. Trondheim: Springer, 2016. DOI https://doi.org/10.1007/978-3-319-45477-1_11. Disponível em: https://link.springer.com/chapter/10.1007/978-3-319-45477-1_11#citeas. Acesso em: maio 2021.

MCCARTHY, C.; HARNETT, K.; CARTER, A. *Characterization of potential security threats in modern automobiles:* A composite modeling approach. Washington: National Highway Traffic Safety Administration, 2014. Disponível em: https://rosap.ntl.bts.gov/view/dot/12119. Acesso em: maio 2021.

MCGUINNESS, D. Ontologies Come of Age. *In:* FENSEL, D. *et al.* (ed.). *The Semantic Web: Why, What, and How.* [*S.l.*]: MIT Press, 2003. p. 171–194.

MOZZAQUATRO, B. *et al*. An Ontology-Based Cybersecurity Framework for the Internet of Things. *Sensors*, v. 18, n. 9, p. 3053-3073, Sep. 2018. DOI 10.3390/s18093053. Disponível em: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6163186/. Acesso em: maio 2021.

MOZZAQUATRO, B.; JARDIM-GONCALVES, R.; AGOSTINHO, C. Towards a reference ontology for security in the internet of things. *In:* IEEE INTERNATIONAL WORKSHOP ON MEASUREMENTS & NETWORKING, 2015, Coimbra. *Proceedings* […]. Portugal: IEEE, 2015. DOI 10.1109/IWMN.2015.7322984. Disponível em: https://ieeexplore.ieee.org/document/7322984. Acesso em: mar. 2021.

PETERSEN, K. *et al.* Systematic Mapping Studies in Software Engineering. *In:* INTERNATIONAL CONFERENCE ON EVALUATION AND ASSESSMENT IN SOFTWARE ENGINEERING, 12., 2008, Italy. *Proceedings* [...]. Italy: University of Bari, 2008. p. 68–77.

RASKIN, V. *et al.* Ontology in information security: a useful theoretical foundation and methodological tool. *In:* WORKSHOP ON NEW SECURITY PARADIGMS, Sep. 2001. *Proceedings* [...]. New Mexico: ACM, 2001. p. 53-59. Disponível em: https://doi.org/10.1145/508171.508180. Acesso em: jan. 2021.

RAZZAQ, A. *et al.* Ontology for attack detection: An intelligent approach to web application security. Computers & Security, v. 45, p. 124-146, Sep. 2014. DOI https://doi.org/10.1016/j.cose.2014.05.005. Disponível em: https://www.sciencedirect.com/science/article/pii/S0167404814000868. Acesso em: jan. 2021.

SCHMITTNER, C. *et al.* Security application of failure mode and effect analysis (FMEA). *In:* INTERNATIONAL CONFERENCE ON COMPUTER SAFETY, RELIABILITY, AND SECURITY, Sep. 2014, Delft, The Netherlands. *Proceedings* […]. Delft: Springer, 2014. DOI https://doi.org/10.1007/978-3-319-10506-2_21. Disponível em: https://link.springer.com/chapter/10.1007/978-3-319-10506-2_21. Acesso em: abr. 2021.

SCHMITTNER, C. *et al.* Using SAE J3061 for Automotive Security Requirement Engineering. *In:* INTERNATIONAL CONFERENCE ON COMPUTER SAFETY, RELIABILITY, AND SECURITY, Sep. 2016, Trondheim, Norway. *Proceedings* […]. Norway: Springer International Publishing, 2016. DOI https://doi.org/10.1007/978-3-319-45480-1_13. Disponível em: https://link.springer.com/chapter/10.1007/978-3-319-45480-1_13. Acesso em: fev. 2021.

SOCIETY OF AUTOMOTIVE ENGINEERS (SAE). Cybersecurity guidebook for cyber-physical automotive systems: SAE J3061. *SAE-Society of Automotive Engineers*, Jan. 2016. Disponível em: https://www.sae.org/standards/content/j3061_201601/. Acesso em: fev. 2021.

TAO, M. *et al*. Multi-layer cloud architectural model and ontology-based security service framework for IoT-based smart homes. *Future Generation Computer Systems*, v. 78, n. 3, p. 1040–1051, Jan. 2018. DOI https://doi.org/10.1016/j.future.2016.11.011. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S0167739X16305775. Acesso em: mar. 2021.

VAN REES, R. Clarity in the usage of the terms ontology, taxonomy and classification. *In:* INTERNATIONAL CONFERENCE ON CONSTRUCTION, 20., 2003, Waiheke Island. *Proceedings* […]. Waiheke Island, New Zealand: CIB w78, 2003. Disponível em: https://www.cs.auckland.ac.nz/research/conferences/w78/papers/W78-37.pdf. Acesso em: maio 2021.

VITAL, L. P.; CAFÉ, L. M. A. Ontologias e taxonomias: diferenças. *Perspectivas em Ciência da Informação*, Belo Horizonte, v. 16, n. 2, p. 115–130, jun. 2011. Disponível em: http://portaldeperiodicos.eci.ufmg.br/index.php/pci/article/view/200. Acesso em: abr. 2021.

WU, S.; ZHANG, Y.; CAO, W. Network security assessment using a semantic reasoning and graph based approach. *Computers & Electrical Engineering*, v. 64, p. 96-109, 2017. DOI https://doi.org/10.1016/j.compeleceng.2017.02.001. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S0045790617302409. Acesso em: mar. 2021.