Threat Modeling Methods in the Medical Device Industry: An Integrative Literature Review

Nadica Hrgarek Lechner, Vjeran Strahonja, Zlatko Stapić
Faculty of Organization and Informatics
University of Zagreb
Pavlinska 2, 42000 Varaždin, Croatia
{nhrgarek, vjeran.strahonja, zstapic}@foi.hr

***Abstract**. Threat modeling is a structured information generating process that begins early in the development life cycle to identify potential security threats to a system being built. Threat modeling for medical devices is a relatively new area of research. The medical device industry recognizes the benefits of performing threat modeling throughout the product life cycle by adopting threat modeling to systematically uncover threats and proactively develop secure medical devices. This paper presents the results of an integrative literature review of 26 relevant studies. A total of 32 threat modeling methods and approaches in the medical device industry were identified and systematized.*

Keywords. attack trees, cybersecurity, integrative literature review, medical devices, medical device industry, STRIDE, threat model, threat modeling, threat modeling methods

1 Introduction

The early beginnings of the study of threats were not in science but industry. In the late 1990s, Microsoft employees Loren Kohnfelder and Praerit Garg published an internal paper that described a taxonomy of threats to software (Kohnfelder, 2022). They named it the S.T.R.I.D.E. security threat model to address six major categories of threats: Spoofing of user identity, Tampering with data, Repudiability, Information disclosure (privacy breach), Denial of Service (D.o.S.), and Elevation of privilege (Kohnfelder & Garg, 1999). Threat modeling has become a crucial element of the Microsoft Security Development Lifecycle (SDL). Microsoft has released the Threat Modeling Tool (“Microsoft Threat Modeling Tool,” 2020) as a free application for Windows to guide the development teams through the threat modeling process using STRIDE.

While threat modeling is commonly used in software development projects as part of a secure development lifecycle (Howard & Lipner, 2006), it is a relatively new topic within the medical device industry. Medical device manufacturers need to design and deliver safe and secure products, and have a long experience with the safety risk management process required by ISO 14971 standard (*ISO 14971: Medical devices – Application of risk management to medical devices*, 2019). However, security risk management in the medical domain is a relatively new topic that was addressed by the FDA (Food and Drug Administration), a federal agency of the United States responsible for protecting public health. FDA (2014) issued the first guidance that specifically addresses the management of cybersecurity in medical devices.

New draft guidance (FDA, 2022, p. 10) recommends threat modeling to be performed as part of the security risk assessment to inform and support the risk analysis activities. In the context of medical devices, threat modeling identifies threats that could adversely impact the safety and security of a medical device (The MITRE Corporation & MDIC, 2021, p. 48). According to the technical information report (*AAMI TIR57: Principles for medical device security–Risk management*, 2019), the first activity of the security risk management process is security risk assessment consisting of security risk analysis and security risk evaluation.

Several cybersecurity guidances (FDA, 2016), (FDA, 2018), (FDA, 2022), (IMDRF, 2020), (MDCG, 2020), (NMPA, 2022), (SFDA, 2019), (TGA, 2021), (“IT Security Guideline for Medical Devices,” 2021), standard (*IEC 81001-5-1: Health software and health IT systems safety, effectiveness and security – Part 5-1: Security – Activities in the product life cycle*, 2021), and other publications (*AAMI TIR57: Principles for medical device security–Risk management*, 2019), (HSCC, 2019), (The MITRE Corporation & MDIC, 2021) for the medical device industry emphasize the importance of threat modeling which can be used as part of security risk assessments.

A threat model should be the output of a systematic approach (Ray, 2021, p. 141) for identifying assets, vulnerabilities, and threats. Unstructured brainstorming sessions and other non-systematic approaches for identifying potential threats and vulnerabilities are not acceptable for medical devices because they cannot produce an exhaustive list of threats.

Threat modeling can be applied to software, devices, systems, networks, distributed systems, and business processes (*IEC 81001-5-1: Health software and health IT systems safety, effectiveness and security – Part 5-1: Security – Activities in the product life cycle*, 2021). According to Shostack (2014, pp. xxiii-xxiv), there are many reasons to use threat modeling: finding security bugs early, understanding security requirements, engineering and delivering better products, and addressing issues other techniques won't find. In the context of software development, Howard & Lipner (2006, p. 102) list the following benefits of threat modeling: contributes to the risk management process because threats to software and infrastructure are risks to the user and environment deploying the software, uncovers threats to the system before the system is committed to code, revalidates the architecture and design by having the development team go over the design again, forces development staff to look at the design from a different viewpoint– that of security and privacy, helps clarify the selection of appropriate countermeasures for the application and environment, contributes to the Attack Surface Reduction (ASR) process for the software, helps guide the code review process, and guides the penetration testing process. When done right, threat modeling can assist cybersecurity professionals, developers, and subject matter experts during the security risk assessment of a medical device.

FDA (2022, p. 11) recommends that premarket submissions include threat modeling documentation and does not prescribe any specific methodology or method for threat modeling. There are many threat modeling methods, whose comprehensive summary is given by Shevchenko et al. (2018), citing STRIDE and associated derivations, PASTA (Process for Attack Simulation and Threat Analysis), attack trees, LINDUN (Linkability, Identifiability, Non-repudiation, Detectability, Disclosure of information, Unawareness, Noncompliance), CVSS (Common Vulnerability Scoring System), persona non grata, security cards, hTMM (Hybrid Threat Modeling Method), Quantitative TMM (Threat Modeling Method), Trike, VAST (Visual, Agile, and Simple Threat) modeling, and OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation). According to (Shevchenko et al., 2018), threat modeling methods are used to create an abstraction of the system, profiles of potential attackers, and a catalog of potential threats that may arise. Three main approaches in threat modeling that help highlight threats that may be present in a system are: system-centric approach, attacker-centric approach, and asset-centric approach (Tarandach & Coles, 2020).

Having the importance of threat modeling explained, the question that arises is what methods and approaches could be used in threat modeling, particularly in the medical device industry. Thus, the purpose of this paper is to present an integrative review of published literature on the different threat modeling methods and approaches in the medical device industry.

The rest of the paper is organized as follows. The research methodology is described in section 2. Section 3 presents the results from the conducted integrative literature review and a discussion of the findings. The final section of the paper restates the research problem, summarizes the findings, discusses the implications, and provides recommendations for future research directions.

2 Methodology

An integrative literature review is a form of research that reviews, critiques, and synthesizes representative literature on a topic in an integrated way such that new frameworks and perspectives on the topic are generated (Torraco, 2005, p. 356). In cases where a research question requires a more creative collection of data, an integrative review approach can be useful when the purpose of the review is not to cover all articles ever published on the topic but rather to combine perspectives and insights from different fields or research traditions (Snyder, 2019).

We followed the integrative literature review methodology proposed by Whittemore & Knafl (2005). In their methodology, the integrative literature review consists of five stages: problem identification, literature search, data evaluation, data analysis, and presentation. The integrative literature review was chosen because it includes research articles, books, and other published texts (Snyder, 2019).

2.1 Problem Identification

Malamas et al. (2021) provide an overview of IoMT (Internet of Medical Things) threat models found in the scientific literature. Vakhter et al. (2022) proposed a domain-specific qualitative-quantitative threat model for miniaturized wireless biomedical devices and compared their proposed model to four other threat models. To the best of the authors' knowledge, a review and synthesis of different threat modeling methods and approaches in the medical device industry does not exist in published literature.

We aim to answer the following research question: Which threat modeling methods and approaches can be used in the medical device industry? To answer the research question, we conducted an integrative literature review.

To get an overview of the research topic, a basic Topic search for the exact phrase "threat modeling" was performed in the Clarivate Analytics' Web of Science Core Collection citation database and returned 356 publications. The search range was from 1955 to August 16th, 2022. The search results were refined by the publication date range as listed in Table 1. Web of Science Core Collection was chosen because every journal and book covered by Web of Science Core Collection is assigned to at least one or more Web of Science categories.

Table 1. Distribution of publications by publication date range

Publication date range	Number of publications	% of 356
2005–2010	14	3.93
2011–2015	73	20.51
2016–2020	189	53.09
2021–16/08/2022	80	22.47
Total	**356**	**100.00**

First publications on threat modeling were published between 2005 and 2010. A significant increase in the number of published publications was noted between 2016 and 2020. This increase may be related to cybersecurity threats which continue to grow year over year. In the time between January 2021 and August 16th, 2022, 80 publications were published and the number is expected to increase over the coming years.

The search results were analyzed according to the Web of Science categories. The top 25 of the total 63 categories are presented and sorted in descending order according to the number of occurrences in Table 2.

Table 2. Distribution of publications by the top 25 of the total 63 Web of Science categories

No.	Web of Science categories	Number of publications	% of 356
1	Computer Science Information Systems	149	41.85
2	Computer Science Theory Methods	132	37.08
3	Engineering Electrical Electronic	91	25.56
4	Computer Science Software Engineering	82	23.03
5	Telecommunications	66	18.54
6	Computer Science Interdisciplinary Applications	29	8.15
7	Computer Science Hardware Architecture	23	6.46
8	Computer Science Artificial Intelligence	22	6.18
9	Engineering Multidisciplinary	11	3.09
10	Automation Control Systems	7	1.97
11	Multidisciplinary Sciences	7	1.97
12	Engineering Industrial	6	1.68
13	Chemistry Analytical	5	1.40
14	Instruments Instrumentation	5	1.40
15	Transportation Science Technology	5	1.40
16	Computer Science Cybernetics	4	1.12
17	Operations Research Management Science	4	1.12
18	Physics Applied	4	1.12
19	Business	3	0.84
20	Construction Building Technology	3	0.84
21	Education Educational Research	3	0.84
22	Education Scientific Disciplines	3	0.84
23	Engineering Civil	3	0.84
24	Engineering Mechanical	3	0.84
25	Medical Informatics	3	0.84

As expected, the first eight ranked categories are related to IT in general, but it is worth mentioning that medical informatics is still not recognized as an important category and only 3 publications are assigned to that category.

2.2 Literature Search

The following types of literature written in English from 2010 to 2022 were included in the integrative review: articles published in conference materials and academic journals, books, guidances, standards, and other professional publications about medical device cybersecurity. The search range was from 2010 because at that time medical device manufacturers increasingly started considering adding or expanding connectivity options for medical devices. From a regulatory point of view, guidance that addresses the management of cybersecurity in medical devices throughout the premarket phase (FDA, 2014) was first published in October 2014. In May 2015, the FDA issued a first safety communication related to reported security vulnerabilities in Hospira's LifeCare PCA3 and PCA5 Infusion Pump Systems ("LifeCare PCA3 and PCA5 Infusion Pump Systems by Hospira: FDA Safety Communication - Security Vulnerabilities," 2015). The search of the literature in electronic databases was performed on April 18, 2022.

The EBSCO Discovery Service (EDS) search engine was used to search for specific terms in full text to identify potential articles: *"((threat modeling) OR (threat modelling) OR (threat model)) AND ((medical device) OR (medical devices) OR (medical IoT devices) OR (medical device software))"*. The search was conducted using the Boolean/Phrase search mode. In addition, the following expanders were applied: full text and equivalent subjects. The search returned 4 studies and 1 duplicate was excluded.

Additional articles were collected using the PubMed and IEEE Xplore search engines. The PubMed database was chosen because it supports the search and retrieval of biomedical and life sciences literature. IEEE Xplore provides full-text access to the technical literature in engineering and technology.

PubMed was searched using the following query: *"((threat modeling) OR (threat modelling) OR (threat model)) AND ((medical device) OR (medical devices) OR (medical IoT devices) OR (medical device software))"* with parameter [Title/Abstract]. The search returned 1 study.

IEEE Xplore advanced search was used to search for search terms *"threat modeling" OR "threat modelling" OR "threat model" AND "medical device"*

OR "medical devices" OR "medical IoT devices" OR "medical device software" in all metadata. The search resulted in a literature set consisting of 87 studies published in the IEEE Xplore digital library from 2010 to 2022.

Grey literature was found by conducting Google searches for documents published on the Internet from January 2010 to May 2022. Google search was performed on May 13th, 2022. The search strategy included the following queries: *threat modeling medical devices*, *threat modeling medical devices filetype:pdf*. Since it is impossible to screen all retrieved results from Google searches, we relied on relevancy ranking within the Google search engine to bring the most relevant results to the top of the list, and limited our search to the first 10 pages of results of each search query. The search results were reviewed using the title and short text underneath to identify the studies that are relevant to the research topic. The websites of organizations issuing standards for medical devices (i.e., IEC, AAMI) were also searched and 2 publications were found. In addition, 2 books about medical devices were screened and found to be eligible for inclusion in the integrative literature review.

2.3 Data Evaluation

The results of the database searches and grey literature searches were exported to an Excel spreadsheet and 2 duplicates were excluded through the 'Remove Duplicates' function. The abstracts and/or full text of all studies were manually reviewed to determine if a study is related to medical devices and threat modeling and if threat modeling methods/approaches are explicitly specified.

A total of 26 relevant studies were included in the present review, as shown in Fig. 1. A variable named "n" stands for the number of studies. The included studies are summarized in Table 3. Primary literature sources relevant to the research topic included 7 journal articles, 8 conference papers, 3 magazine articles, and 1 early access article. 7 out of 26 included studies represent grey literature including other types of non-journal literature such as books, playbooks, guidances, whitepapers, standards, and technical information reports.

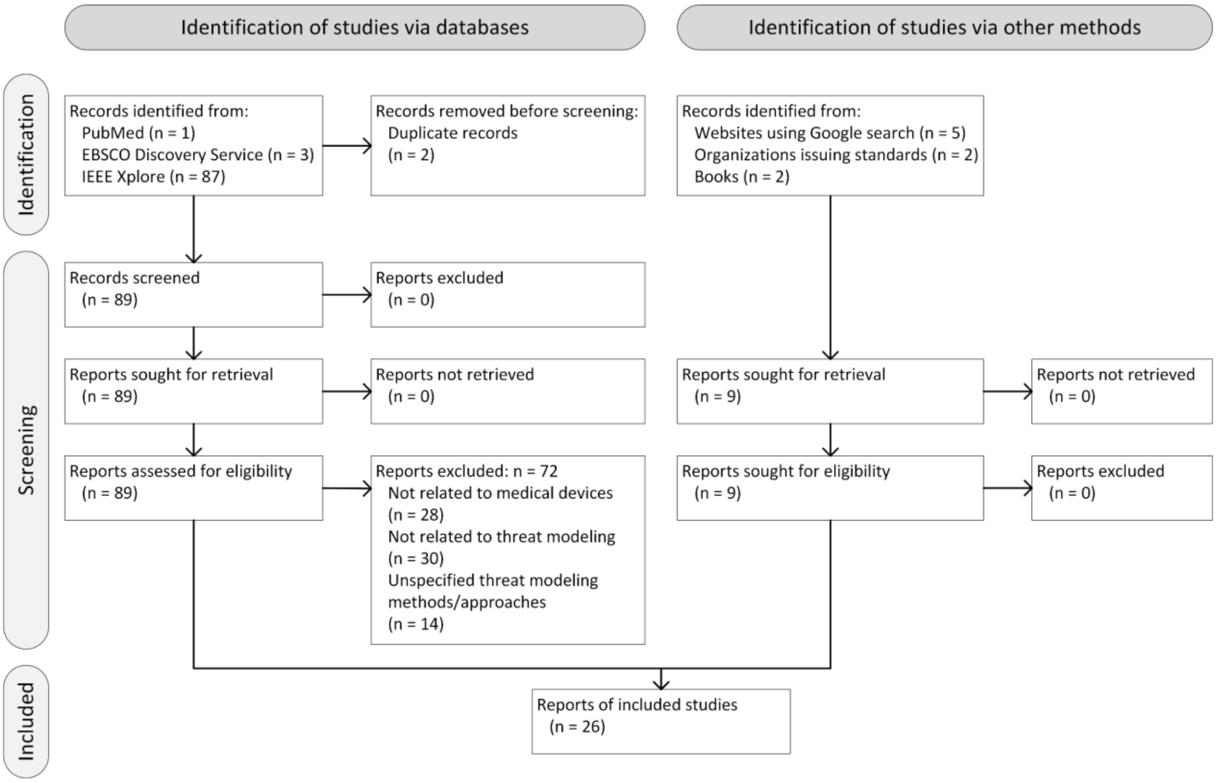
Identification of studies via databases
Identification of studies via other methods
Identification
Screening
Included
Records identified from: PubMed (n = 1) EBSCO Discovery Service (n = 3) IEEE Xplore (n = 87)
Records removed before screening: Duplicate records (n = 2)
Records identified from: Websites using Google search (n = 5) Organizations issuing standards (n = 2) Books (n = 2)
Records screened (n = 89)
Reports excluded (n = 0)
Reports sought for retrieval (n = 89)
Reports not retrieved (n = 0)
Reports sought for retrieval (n = 9)
Reports not retrieved (n = 0)
Reports assessed for eligibility (n = 89)
Reports excluded: n = 72 Not related to medical devices (n = 28) Not related to threat modeling (n = 30) Unspecified threat modeling methods/approaches (n = 14)
Reports sought for eligibility (n = 9)
Reports excluded (n = 0)
Reports of included studies (n = 26)

Figure 1. Flow diagram of studies screened through the review process

2.4 Data Analysis

The included studies were categorized according to the study type, device type, and threat modeling methods/approaches. It was interesting to see that some studies have focused on a particular medical device type such as an implantable pacemaker or similar, while the vast majority of studies have focused on a broader range of devices referred to as "medical devices" or a little bit more specific but still general enough such as "interoperable medical devices" or "telecare medical information systems". The comprehensive results displaying studies, their types, targeted devices, and identified threat modeling methods or approaches are presented in Table 3.

Table 3. Studies included in the integrative review

Source	Study	Study type	Device type	Threat modeling methods/approaches
PubMed	(Ibrahim et al., 2020)	Journal article	Implantable pacemaker	Attack graphs
EBSCO Discovery Service	(Malamas et al., 2021)	Journal article	Internet of Medical Things (IoMT)	Adversarial model Asset-based Attack paths Attack/defense tree HMG IS1 Logic decision diagram STRIDE STRIDE/DREAD
IEEE Xplore	(Xu et al., 2016)	Conference paper	Interoperable medical devices	Attack trees
	(Roy et al., 2018)	Journal article	E-healthcare systems	Dolev–Yao threat model
	(Kim et al., 2020)	Journal article	Medical devices	Attack trees
	(Manikandan & Sathyadevan, 2021)	Conference paper	Medical Implant Communication Systems (MICS) network	Attack trees
	(Almohri et al., 2017)	Conference paper	Medical cyber physical systems	Attack trees Attacker-centric model System-centric model
	(Lei & Chuang, 2019)	Journal article	Telecare medical information systems	Adversarial model
	(Shen et al., 2019)	Magazine article	Medical image retrieval for MIoT (Medical Internet of Things)	STRIDE derivation
	(Liu et al., 2020)	Journal article	Crowdsourcing IoT (Internet of Things)	Dolev-Yao threat model
	(Venkatasubramanian et al., 2012)	Magazine article	Interoperable medical devices	Attack classes
	(Vasserman et al., 2012)	Magazine article	Interoperable medical devices	Attack-consequences model with attack scenarios
	(Alsuwaidi et al., 2020)	Conference paper	Medical devices	Ways of attacks
	(Vakhter et al., 2022)	Early access article	Miniaturized wireless biomedical devices	Domain-specific qualitative-quantitative threat model
	(Cagnazzo et al., 2018)	Conference paper	Mobile health systems	DREAD STRIDE
	(Atamli & Martin, 2014)	Conference paper	IoT (smart healthcare system use case)	STRIDE derivation
	(Ould-Yahia et al., 2018)	Conference paper	e-Health in IoT-cloud environment	Adversary model
Google search	(The MITRE Corporation & MDIC, 2021)	Playbook	Medical devices	ATT&CK framework Attack trees Cyber Attack Lifecycle DREAD NIST SP 800-30 Appendices D-I Rubric for applying CVSS to Medical Devices STRIDE
	(Medcrypt, 2020)	Whitepaper	Medical devices	Attack trees CVSS PASTA Rubric for applying CVSS to Medical Devices

Source	Study	Study type	Device type	Threat modeling methods/approaches
				STRIDE
	(Seifert & Reza, 2016)	Journal article	Cyber-physical systems for healthcare	STRIDE DREAD
	(TGA, 2021)	Guidance	Medical devices	ATT&CK framework
	(Seale et al., 2018)	Conference paper	Networked medical devices	CVE (Common Vulnerabilities and Exposures) CVSS CWE (Common Weakness Enumeration) NVD (National Vulnerability Database) STRIDE
Organizations issuing standards	(*AAMI TIR57: Principles for medical device security–Risk management*, 2019)	Technical information report	Medical devices	Attack trees CVSS Security risk assessment approaches (threat-oriented, asset/impact-oriented, vulnerability-oriented)
	(*IEC 81001-5-1: Health software and health IT systems safety, effectiveness and security – Part 5-1: Security – Activities in the product life cycle*, 2021)	Standard	Health software, health IT systems	Attack-defense trees CAPEC dictionary of known patterns of attack CWE/SANS Top 25 Most Dangerous Software Errors CWSS (Common Weakness Scoring System) DREAD List known potential vulnerabilities OCTAVE OWASP Top 10 STRIDE Trike VAST
Book	(Ray, 2021)	Book	Medical devices	Attack tree CBOM (Cybersecurity Bill of Materials) CVSS Rubric for applying CVSS to Medical Devices STRIDE
	(Wirth et al., 2020)	Book	Medical devices	STRIDE

2.5 Presentation

The results of the integrative review are presented in Fig. 2. These results indicate that most methods have not stepped out of scientific laboratories into a wider professional application. Similar to other areas, in addition to the inherent quality of the method, it is crucial whether there are computer tools based on the method.

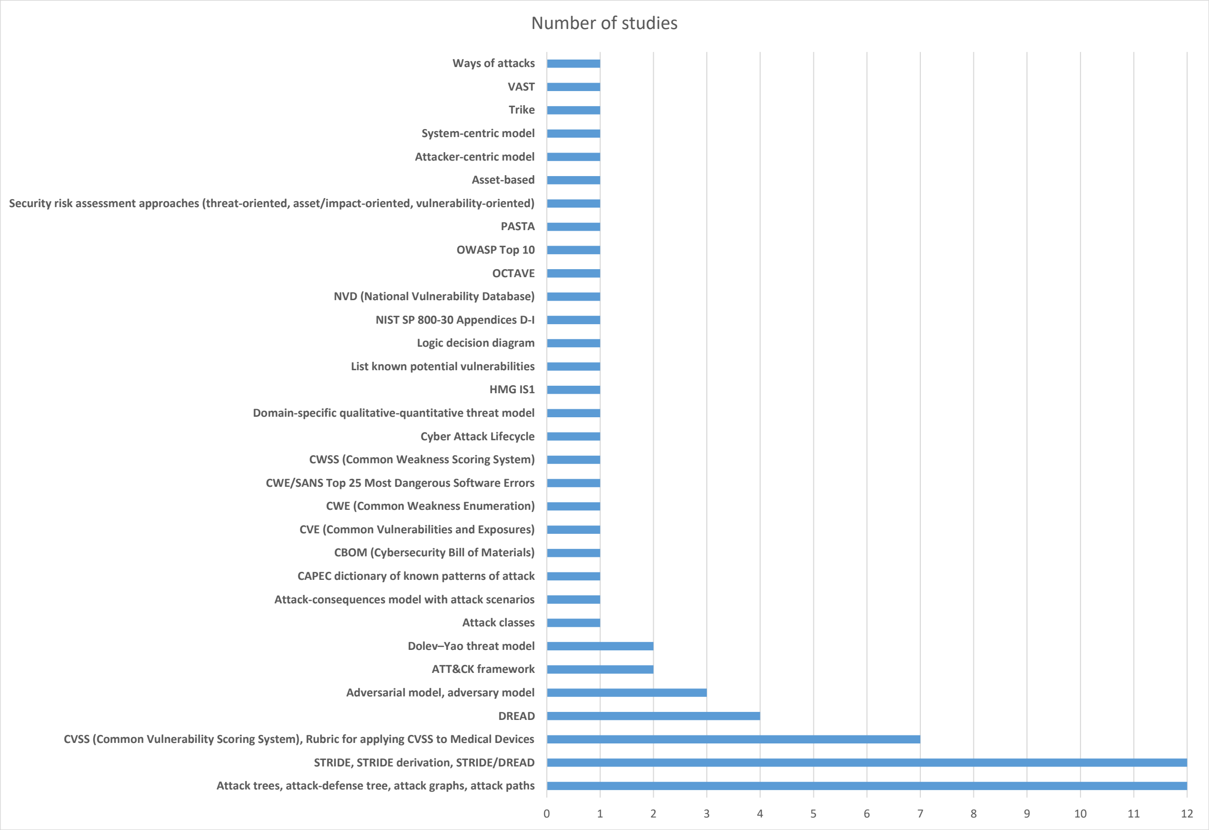

Figure 2. Number of studies per identified threat modeling method/approach

3 Discussion on Results

Our research identified a total of 32 threat modeling methods and approaches in the medical device industry. As illustrated in Fig. 2, the integrative literature review identified that 75% of threat modeling methods and approaches are not reported to be used outside the laboratory of the researchers presenting it. Although hurtful, the results also show the importance of this topic being actively researched over the course of past years.

Attack trees and the STRIDE threat taxonomy, including their derivations, appear to be the most used threat modeling methods. CVSS, Rubric for applying CVSS to Medical Devices and DREAD are the most used approaches for vulnerability scoring and to support the calculation of security risks. Threat catalogs based on NVD, CVE, CWE, ATT&CK framework and CAPEC dictionary of known patterns of attack can be used to derive further attack vectors to which a medical device may be subjected. Other approaches such as the OWASP Top 10, CWE/SANS TOP 25 Most Dangerous Software Errors, and NIST SP 800-30 Appendices D-I can be used to support threat modeling and security risk assessments.

Two studies (Roy et al., 2018), (Liu et al., 2020) included the Dolev-Yao threat model (Dolev & Yao, 1983) that can be used to analyze the security of public key protocols against saboteurs. The Dolev-Yao threat model was not mentioned in grey literature. It should be noted that grey literature provided examples of other threat modeling methods which were not found in the primary literature. Two studies (Almohri et al., 2017), (*AAMI TIR57: Principles for medical device security–Risk management*, 2019) also included approaches to threat modeling such as attacker-centric, asset-centric, and threat-centric. Five studies mentioned the DREAD (Damage potential, Reproducibility, Exploitability, Affected users, Discoverability) risk assessment technique. In the past, Microsoft used DREAD ratings to calculate security risk (Howard & Lipner, 2006). Three studies mentioned the technical paper (The MITRE Corporation, 2020) about a rubric for applying CVSS to medical devices.

3.1 Research Limitations

There may be some possible limitations in the present research. The first is a literature gap due to the lack of previous research on the topic. The second limitation concerns the manual review of studies to identify if a study is related to medical devices and threat modeling, and which threat modeling methods/approaches are specified. The third limitation is related to data collection. The research included studies presented in one language and there is no guarantee that all relevant grey literature was retrieved from the search.

4 Conclusions

Threat modeling is an integral part of a secure medical device product development life cycle. This paper presents the results of an integrative literature review of published studies on the different threat modeling methods in the medical device industry. Although further investigations are needed, the present research contributes to the existing literature on the topic of threat modeling methods and approaches in the medical device industry.

This paper may assist security professionals, threat modeling experts, security risk managers, software/firmware developers, subject matter experts, and other stakeholders who participate in threat modeling activities of medical devices to choose a specific threat modeling method and embrace threat modeling throughout the medical device life cycle.

The studies were collected using the following search engines: PubMed, EDS, and IEEE Xplore. Future research could conduct literature searches in other academic research databases such as Web of Science, Scopus, SpringerLink, SAGE journals, or ScienceDirect.

Further investigation should explore the advantages and disadvantages of identified threat modeling methods and approaches and which threat modeling tools are recommended for medical device threat modeling. More research is needed to explore if threat modeling is carried out not just for new medical devices, but also on legacy devices. Future research should also investigate if the TARA (Threat Agent Risk Assessment) methodology (Rosenquist, 2009) can be adapted for the medical device industry.

Acknowledgments

The authors would like to thank the anonymous reviewers for their valuable comments and suggestions that significantly improved this paper.

References

AAMI TIR57: Principles for medical device security–Risk management. (2019).

Almohri, H., Cheng, L., Yao, D., & Alemzadeh, H. (2017). On Threat Modeling and Mitigation of Medical Cyber-Physical Systems. *Proceedings of the 2017 IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE)*, Philadelphia, (pp. 114–119). IEEE. doi:10.1109/CHASE.2017.69

Alsuwaidi, A., Hassan, A., Alkhatri, F., Ali, H., Qbea'H, M., & Alrabaee, S. (2020). Security Vulnerabilities Detected in Medical Devices. *Proceedings of the 2020 12th Annual Undergraduate Research Conference on Applied Computing (URC)*, Dubai, (pp. 1–6). IEEE. doi:10.1109/URC49805.2020.9099192

Atamli, A. W., & Martin, A. (2014). Threat-Based Security Analysis for the Internet of Things. *Proceedings of the 2014 International Workshop on Secure Internet of Things*, Wroclaw, (pp. 35–43). IEEE. doi:10.1109/SIoT.2014.10

Cagnazzo, M., Hertlein, M., Holz, T., & Pohlmann, N. (2018). Threat modeling for mobile health systems. *Proceedings of the 2018 IEEE Wireless Communications and Networking Conference Workshops (WCNCW)*, Barcelona, (pp. 314–319). IEEE. doi:10.1109/WCNCW.2018.8369033

Dolev, D., & Yao, A. C. (1983). On the Security of Public Key Protocols. *IEEE Transactions on Information Theory*, 29(2), 198–208. doi:10.1109/TIT.1983.1056650

FDA. (2014). Content of Premarket Submissions for Management of Cybersecurity in Medical Devices – Guidance for Industry and Food and Drug Administration Staff. Retrieved from https://www.fda.gov/media/86174/download

FDA. (2016). Postmarket Management of Cybersecurity in Medical Devices – Guidance for Industry and Food and Drug Administration Staff. Retrieved from https://www.fda.gov/media/95862/download

FDA. (2018). Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions – Draft Guidance for Industry and Food and Drug Administration Staff. Retrieved from https://www.fda.gov/media/119933/download

FDA. (2022). Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions – Draft Guidance for Industry and Food and Drug Administration Staff. Retrieved from https://www.fda.gov/media/119933/download

Howard, M., & Lipner, S. (2006). *The Security Development Lifecycle. SDL: A Process for Developing Demonstrably More Secure Software*. Redmond: Microsoft Press.

HSCC. (2019). Medical Device and Health IT Joint Security Plan. Retrieved from https://healthsectorcouncil.org/wp-content/uploads/2019/02/HSCC-MEDTECH-JSP-v1.2.pdf

Ibrahim, M., Alsheikh, A., & Matar, A. (2020). Attack Graph Modeling for Implantable Pacemaker. *Biosensors*, 10(2), 14. doi:10.3390/bios10020014

IEC 81001-5-1: Health software and health IT systems safety, effectiveness and security – Part 5-1: Security – Activities in the product life cycle. (2021).

IMDRF. (2020). Principles and Practices for Medical Device Cybersecurity. Retrieved from https://www.imdrf.org/sites/default/files/docs/imdrf/final/technical/imdrf-tech-200318-pp-mdc-n60.pdf

ISO 14971: Medical devices – Application of risk management to medical devices. (2019).

IT Security Guideline for Medical Devices. (2021). Retrieved from https://github.com/johner-institut/it-security-guideline/blob/master/Guideline-IT-Security_EN.md

Kim, D., Choi, J., & Han, K. (2020). Medical Device Safety Management Using Cybersecurity Risk Analysis. *IEEE Access*, 8, 115370–115382. doi:10.1109/ACCESS.2020.3003032

Kohnfelder, L. (2022). *Designing Secure Software: A Guide for Developers*. San Francisco: No Starch Press.

Kohnfelder, L., & Garg, P. (1999). The threats to our products. Retrieved from https://adam.shostack.org/microsoft/The-Threats-To-Our-Products.docx

Lei, C.-L., & Chuang, Y.-H. (2019). Privacy Protection for Telecare Medicine Information Systems with Multiple Servers Using a Biometric-based Authenticated Key Agreement Scheme. *IEEE Access*, 7, 186480–186490. doi:10.1109/ACCESS.2019.2958830

LifeCare PCA3 and PCA5 Infusion Pump Systems by Hospira: FDA Safety Communication - Security Vulnerabilities. (2015). Retrieved from https://wayback.archive-it.org/7993/20170112164109/http:/www.fda.gov/Safety/MedWatch/SafetyInformation/SafetyAlertsforHumanMedicalProducts/ucm446828.htm

Liu, W., Wang, X., & Peng, W. (2020). Secure Remote Multi-Factor Authentication Scheme Based on Chaotic Map Zero-Knowledge Proof for Crowdsourcing Internet of Things. *IEEE Access*, 8, 8754–8767. doi:10.1109/ACCESS.2019.2962912

Malamas, V., Chantzis, F., Dasaklis, T. K., Stergiopoulos, G., Kotzanikolaou, P., & Douligeris, C. (2021). Risk Assessment Methodologies for the Internet of Medical Things: A Survey and Comparative Appraisal. *IEEE Access*, 9, 40049–40075. doi:10.1109/ACCESS.2021.3064682

Manikandan, R., & Sathyadevan, S. (2021). Medical Implant Communication Systems (MICS) Threat Modelling. *Proceedings of the 2021 2nd International Conference on Secure Cyber Computing and Communications (ICSCCC)*, Jalandhar, (pp. 518–523). IEEE. doi:10.1109/ICSCCC51823.2021.9478155

MDCG. (2020). MDCG 2019-16 Rev.1 Guidance on Cybersecurity for medical devices. Retrieved from https://ec.europa.eu/health/document/download/b23b362f-8a56-434c-922a-5b3ca4d0a7a1_en?filename=md_cybersecurity_en.pdf

Medcrypt. (2020). *Medical device threat modeling* [White paper]. Retrieved from https://www.medcrypt.co/whitepaper_resources/WP9_Medical%20Device%20Threat%20Modeling_v4.1.pdf

Microsoft Threat Modeling Tool. (2020). Retrieved from https://docs.microsoft.com/en-us/azure/security/develop/threat-modeling-tool

NMPA. (2022). Guidelines for Registration Review of Medical Device Cybersecurity (Revised Edition 2022).

Ould-Yahia, Y., Bouzefrane, S., & Boucheneb, H. (2018). Towards privacy and ownership preserving of outsourced health data in IoT-cloud context. *Proceedings of the 2018 International Symposium on Programming and Systems (ISPS)*, Algiers, (pp. 1–6), doi:10.1109/ISPS.2018.8379018

Ray, A. (2021). *Cybersecurity for Connected Medical Devices*. Eastbourne: Academic Press.

Rosenquist M. (2009). *Prioritizing Information Security Risks with Threat Agent Risk Assessment* [White paper]. Retrieved from https://media10.connectedsocialmedia.com/intel/10/5725/Intel_IT_Business_Value_Prioritizing_Info_Security_Risks_with_TARA.pdf

Roy, S., Chatterjee, S., Das, A. K., Chattopadhyay, S., Kumari, S., & Jo, M. (2018). Chaotic Map-Based Anonymous User Authentication Scheme With User Biometrics and Fuzzy Extractor for Crowdsourcing Internet of Things. *IEEE Internet of Things Journal*, 5(4), 2884–2895. doi:10.1109/JIOT.2017.2714179

Seale, K. A., McDonald, J. T., & Glisson, W. B. (2018). MedDevRisk: Risk Analysis Methodology for Networked Medical Devices. *Proceedings of the 51st Hawaii International Conference on System Sciences (HICSS)*, Hawaii, (pp. 3271–3280). doi:10.24251/HICSS.2018.414

Seifert, D., & Reza, H. (2016). A Security Analysis of Cyber-Physical Systems Architecture for Healthcare. *Computers*, 5(4), 27. doi:10.3390/computers5040027

SFDA. (2019). Guidance to Post-Market Cybersecurity of Medical Devices. Retrieved from https://beta.sfda.gov.sa/sites/default/files/2021-01/MDS-G37.pdf

Shen, M., Deng, Y., Zhu, L., Du, X., & Guizani, N. (2019). Privacy-Preserving Image Retrieval for Medical IoT Systems: A Blockchain-Based Approach. *IEEE Network*, 33(5), 27–33. doi:10.1109/MNET.001.1800503

Shevchenko, N., Chick, T., A., O'Riordan, P., Scanlon, T. P., & Woody, C. (2018). Threat Modeling: A Summary of Available Methods. Retrieved from https://resources.sei.cmu.edu/asset_files/WhitePaper/2018_019_001_524597.pdf

Shostack, A. (2014) *Threat Modeling: Designing for Security*. Indianapolis: John Wiley & Sons.

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, 104, 333–339. doi:10.1016/j.jbusres.2019.07.039

Tarandach, I., & Coles, M. J. (2020). *Threat Modeling: A Practical Guide for Development Teams*. Sebastopol: O'Reilly Media.

TGA. (2021). Medical device cyber security guidance for industry. Retrieved from https://www.tga.gov.au/sites/default/files/medical-device-cyber-security-guidance-industry.pdf

The MITRE Corporation & MDIC. (2021). Playbook for Threat Modeling Medical Devices. Retrieved from https://www.mitre.org/sites/default/files/publications/Playbook-for-Threat-Modeling-Medical-Devices.pdf

The MITRE Corporation. (2020). Rubric for applying CVSS to Medical Devices. Retrieved from https://www.mitre.org/sites/default/files/publications/pr-18-2208-rubric-for-applying-cvss-to-medical-devices.pdf

Torraco, R. J. (2005). Writing integrative literature reviews: Guidelines and examples. *Human Resource Development Review*, 4(3), 356–367. doi:10.1177/1534484305278283

Vakhter, V., Soysal, B., Schaumont, P., & Guler, U. (2021). Security for Emerging Miniaturized Wireless Biomedical Devices: Threat Modeling with Application to Case Studies. *IEEE Internet of Things Journal*. Advanced online publication. doi:10.1109/JIOT.2022.3144130

Vakhter, V., Soysal, B., Schaumont, P., & Guler, U. (2022). Threat Modeling and Risk Analysis for Miniaturized Wireless Biomedical Devices. *IEEE Internet of Things Journal*. Advanced online publication. doi:10.1109/JIOT.2022.3144130

Vasserman, E. Y., Venkatasubramanian, K. K., Sokolsky, O., & Lee, I. (2012). Security and Interoperable-Medical-Device Systems, Part 2: Failures, Consequences, and Classification. *IEEE Security & Privacy*, 10(6), 70–73. doi:10.1109/MSP.2012.153

Venkatasubramanian, K. K., Vasserman, E. Y., Sokolsky, O., & Lee, I. (2012). Security and Interoperable-Medical-Device Systems, Part 1. *IEEE Security & Privacy*, 10(5), 61–63. doi:10.1109/MSP.2012.128

Whittemore, R., & Knafl, K. (2005). The integrative review: updated methodology. *Journal of Advanced Nursing*, 52(5), 546–553. doi:10.1111/j.1365-2648.2005.03621.x

Wirth, A., Gates, C., & Smith, J. (2020). *Medical Device Cybersecurity for Engineers and Manufacturers*. Norwood: Artech House.

Xu, J., Venkatasubramanian, K. K., & Sfyrla, V. (2016). A methodology for systematic attack trees generation for interoperable medical devices. *Proceedings of the 2016 Annual IEEE Systems Conference (SysCon)*, Orlando, (pp. 1–7). IEEE. doi:10.1109/SYSCON.2016.7490632