Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Threat modeling – A systematic literature review

Wenjun Xiong, Robert Lagerström*

Division of Network and Systems Engineering, School of Electrical Engineering and Computer Science, KTH Royal Institute of Technology, Malvinas väg 6, SE-100 44 Stockholm, Sweden

ARTICLE INFO

Article history:
Received 2 July 2018
Revised 8 February 2019
Accepted 12 March 2019
Available online 15 March 2019

Keywords:
Threat modeling
Literature review
Cyber security
Risk management
Cyber attacks

ABSTRACT

Cyber security is attracting worldwide attention. With attacks being more and more common and often successful, no one is spared today. Threat modeling is proposed as a solution for secure application development and system security evaluations. Its aim is to be more proactive and make it more difficult for attackers to accomplish their malicious intents. However, threat modeling is a domain that lacks common ground. What is threat modeling, and what is the state-of-the-art work in this field? To answer these questions, this article presents a review of threat modeling based on systematic queries in four leading scientific databases. This is the first systematic literature review on threat modeling to the best of our knowledge. 176 articles were assessed, and 54 of them were selected for further analysis. We identified three separate clusters: (1) articles making a contribution to threat modeling, e.g., introducing a new method, (2) articles using an existing threat modeling approach, and (3) introductory articles presenting work related to the threat modeling process. The three clusters were analyzed in terms of a set of criteria, for instance: Is the threat modeling approach graphical or formal? Is it focused on a specific attack type and application? Is the contribution validated empirically or theoretically? We observe from the results that, most threat modeling work remains to be done manually, and there is limited assurance of their validations. The results can be used for researchers and practitioners who want to know the state-of-the-art threat modeling methods, and future research directions are discussed.

1. Introduction

Cyber security is a fundamental aspect of networks, computers, software, and data. Without sufficient security, these assets will be vulnerable to malicious threats. The year 2017 saw some of the biggest cyberattacks in recent history,[1] with millions of consumers and thousands of businesses affected by everything from the WannaCry[2] attack to the Equifax[3] and Uber[4] data breaches. Therefore, due to the security requirements of software applications and systems, as well as with the growing use and dependence of IT infrastructure and with it the growing attack surfaces and increasing number of threats, it is of paramount importance to be more proactive

* Corresponding author.
E-mail addresses: wenjx@kth.se (W. Xiong), robertl@kth.se (R. Lagerström).

[1] https://www.csoonline.com/article/3241766/cyber-attacks-espionage/top-5-cybersecurity-concerns-for-2018.html.

[2] https://www.csoonline.com/article/3227906/ransomware/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html.

[3] https://www.wired.com/story/equifax-breach-no-excuse/.

[4] https://www.theguardian.com/technology/2017/nov/29/uber-security-breach-london-sadiq-khan-users.

https://doi.org/10.1016/j.cose.2019.03.010

working with security, instead of only focusing on putting out fires.[5]

As a significant part of cyber security, threat modeling is becoming widespread in application development and system evaluation. However, there has been no systematic literature review on this topic. To fill this gap, this article presents a review of cyber security threat modeling. The aim of this work is to make it easier for researchers and practitioners to get an overview of the threat modeling state-of-the-art, as well as finding possible directions for further research.

To get a reasonable cover of the literature on cyber security threat modeling, systematic queries were conducted using four leading scientific databases. The search results provided us with 176 articles without overlap, and 54 articles were selected for further classification and analysis. The contributions of this work are threefold:

- We provide the first systematic literature review on cyber security threat modeling.
- We provide insight into threat modeling methods and how these methods could be employed and evaluated.
- We provide future research directions for threat modeling.

The rest of this article is structured as follows: Section 2 describes the related work regarding systematic literature reviews within security. Section 3 outlines the review methodology used in this work and the process. Section 4 provides results of the found literature. Based on the results, findings and research directions for future work are discussed in Section 5. Finally, we conclude the article in Section 6.

2. Related work

There is a number of reviews focusing on certain sub-communities within security, e.g., cyber situational awareness (Franke and Brynielsson, 2014), security development models (Shuaibu et al., 2015), cross-site scripting (Hydara et al., 2015), information security management (Soomro et al., 2016), security awareness (Lebek et al., 2013), information security policy compliance (Sommestad et al., 2014), security and privacy in health (Fernández-Alemán et al., 2013), cloud computing risk (Latif et al., 2014), digital forensics (Alharbi et al., 2011), and security requirements engineering (Mellado et al., 2010). However, so far there is no systematic literature review on threat modeling. In this related work section, we describe the findings of the above-mentioned literature reviews in cyber security.

Franke and Brynielsson (2014) conducted s systematic review of 102 research papers in cyber situational awareness and separated the literature into four broad categories, and the key finding is that more empirical research should be conducted.

Shuaibu et al. (2015) conducted a systematic literature review to investigate various security development models, the stages in the development models, as well as the tools and mechanism used to detect vulnerabilities.

Concerned with cross-site scripting, Hydara et al. (2015) identified the solutions and techniques of them. They addressed that there is no single solution that can effectively mitigate cross-site scripting attacks, and more research is needed in the area of vulnerability removal from the source code of the applications before deployment.

Focused on information security, Soomro et al. (2016) synthesized literature related to management's roles to explore specific managerial activities to enhance information security management. Also, Lebek et al. (2013) presented a theory-based literature review of the extant approaches used within employees' information security awareness and behavior. Moreover, to identify variables that influence compliance with information security policies of organizations, Sommestad et al. (2014) investigated 61 variables in relation to peoples' attitudes, intentions or actual behavior. They found that each of the variables only explain a small part of the variation in people's behavior, and when a variable has been investigated in multiple studies the findings often show a considerable variation.

To identify and analyze critical privacy and security aspects of electronic health record systems, Fernández-Alemán et al. (2013) conducted a systematic literature review concerning security and privacy in electronic health records. They addressed that although the design of standards and the promulgation of directives concerning security and privacy have been done, more work should adopt these regulations and to deploy secure electronic health record systems.

For helping cloud users or business organizations to have an overview of the risk factors in a cloud environment, Latif et al. (2014) presented a systematic literature review in the field of cloud computing with a focus on risk assessment, they also suggested possible security measures to help in mitigating the identified risks.

For investigating anti-forensics methods, as well as promote automation of the live investigation, Alharbi et al. (2011) proposed a proactive and reactive functional process, and compared to the active component in the multi-component process. They addressed that all phases in the proactive component of the new process are meant to be automated.

As very few reviews focused on security requirements engineering in a systematic, thorough and unbiased manner, Mellado et al. (2010) conducted a systematic review of security requirements engineering to summarize the evidence regarding this issue, which can provide a background in which to appropriately position new research activities.

The above review work focused on sub-communities within security, however, to the best of our knowledge, there is no systematic literature review on threat modeling, therefore, this article aims to fill this gap.

3. Review methodology and process

This systematic literature review was performed based on the guidelines provided by Booth et al. (2012), Kitchenham (2007), and Okoli and Schabram (2011); the method is similar to the literature review by Franke and Brynielsson (2014). The process of our literature review is shown in Fig. 1. Firstly,

[5] https://www.energydigital.com/power-generation/building-smart-grid-digital-chickens-and-cyber-secure-eggs.

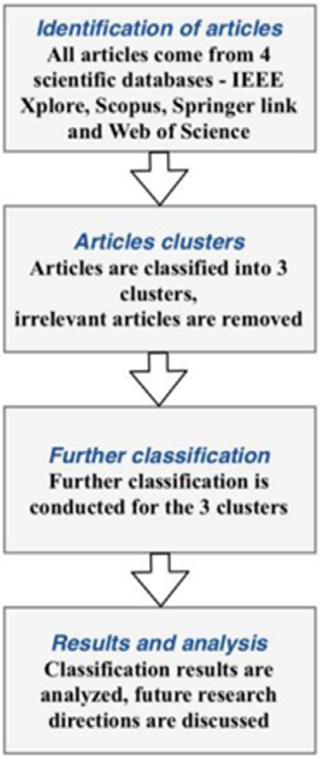
Identification of articles
All articles come from 4 scientific databases - IEEE Xplore, Scopus, Springer link and Web of Science
Articles clusters
Articles are classified into 3 clusters,
irrelevant articles are removed
Further classification
Further classification is conducted for the 3 clusters
Results and analysis
Classification results are analyzed, future research directions are discussed

Fig. 1 – The literature review process employed in this study.

we searched for threat modeling articles in cyber security literature, then we selected and assessed these articles, after which we made further classification and analysis to get detailed information about the selected articles.

To get a reasonable cover of the literature on threat modeling, literature searches were conducted in February 2018, and checked in June 2018, by using four key scientific databases - IEEE Xplore,[6] Scopus,[7] Springer link,[8] and Web of Science.[9] In each case, the search term “threat model”, “threat modeling,” and “threat modeling” with quotation marks were entered within Title-Abstract-Keywords, and refined by topic – “cyber security” or “network security” or “IT security” or “ICT security” or “information security”. To synchronize the search query in the four databases, for IEEE Xplore, we used “Command Search” and searched in “Metadata[10] Only”; for Scopus, we used “Advanced Search” and searched within “TITLE-ABS-KEY”; for Springer link, as there were no blanks for searching within Title-Abstract-Keywords, we manually chosen articles from the search results which contain “threat model” or “threat modeling” or “threat modeling” in title or abstract or keywords; for Web of Science, we used “Advanced Search”, and searched within “Topic”. Moreover, for all the four databases, we defined the document type as “article”, with no time limitation, and only focused on journal publications and discarded conference proceedings.

Running the above search queries, we got the following results:

- IEEE Xplore: 55 articles
- Scopus: 108 articles
- Springer link: 36 articles
- Web of Science: 77 articles

Combined the results of the four databases, we got 176 articles without overlap, as many articles were found several times in different databases. After which an initial classification for these articles was conducted, and a number of articles were removed by answering the following questions:

- Did the article employ or propose a threat model?
- Did the article make a contribution to threat modeling?
- Is the article a threat modeling process article?
- Is the article written in English?

The first three questions only need one answer to be “Yes”, and the fourth question requires a “Yes” answer. Then, 122 articles were removed from further consideration when manually screened, and some common characteristics were identified: (1) Some articles just assumed ad-hoc threat models for specific attack scenarios, e.g., Zhu et al. (2010) assumed that the attacker uses a classical timing analysis attack, and Park et al. (2018) assumed an attacker infects a legitimate client and infiltrates a network, but threat models were not employed or proposed in these articles. (2) Some articles just assumed an attacker’s capability (e.g., Zawoad et al., 2016; Do et al., 2016), without using threat modeling. (3) Some articles just discussed potential attacks (e.g., Shin et al., 2011; Cucurull et al., 2012), without making a contribution to threat modeling. All in all, 54 articles were subject to further analysis.

4. Results

This section aims to analyze state-of-the-art threat modeling articles, in terms of general information (including publication year, author affiliations, outlets, and number of citations), type of threat modeling methods it employed, the aimed system, type of threats and attacks it intended to evaluate, the focus and approach, as well as type of methods the article used in terms of validation.

The selected 54 articles were classified into three clusters:

- Cluster 1 (C1): Applying threat modeling (29 articles)
- Cluster 2 (C2): Threat modeling methods (20 articles)
- Cluster 3 (C3): Threat modeling process (5 articles)

4.1. *General information*

In this subsection, we analyze the general information of the selected articles based on the following aspects:

- Year of publication
- Author affiliation
- Outlet
- Citations

[6] ieeexplore.ieee.org/.
[7] www.scopus.com/.
[8] link.springer.com/.
[9] www.webofknowledge.com/.
[10] Metadata includes abstract and title text and indexing terms.

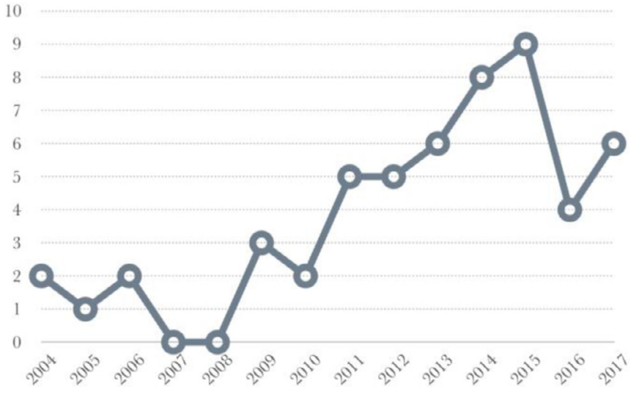

Fig. 2 – The number of threat modeling articles per year.

Table 1 – Number of threat modeling articles from different continents.

Continent	Number of articles
North America	19
Europe	17
Asia Pacific	17
Latin America	1

4.1.1. *Year of publication*

The number of articles per year can be seen as a representation of the research effort in a certain field. The trend for threat modeling research is shown in Fig. 2.

It is fairly easy to see, there is a positive trend in the number of threat modeling articles per year between 2008 and 2015, with a drop in 2016 followed by a higher number again in 2017, although less than the top year of 2015.

4.1.2. *Author affiliation*

The number of articles originating from different continents is displayed in Table 1, note that the co-authors affiliations were also taken into account.

We can infer from Table 1 that, the research on threat modeling is attracting worldwide attention. Among which, the largest portion is from North America, but closely followed by Europe and Asia Pacific. Moreover, the affiliations of authors are widely spread, among which the following three universities appeared more than once: North Dakota State University (Xu and Nygard, 2006; Seifert and Reza, 2016), University of California (Pei et al., 2004; Cardenas et al., 2009), and University of Oxford (Basin et al., 2015; Martina et al., 2015).

4.1.3. *Outlets*

Analyzing the variety of publication outlets can help researchers and practitioners to know where should they submit their work (since there is no Journal of Threat Modeling yet), and where similar research can be found. The publication outlets that appeared more than twice can be seen in Table 2.

The selected articles in this study have been published in several different journals, with IEEE Security & Privacy coming out on top with four articles.

4.1.4. *Citations*

In this section, we study the five most cited articles, as this can help us assess the potential research impact of threat modeling articles. We adapted Google Scholar Citation Index as a unified measurement, and the results are shown in Table 3.

The largest number of citations (183) was acquired by Deng et al. (2011), who claimed that privacy is being seriously threatened by the lack of proper legislation on how information may be collected, processed, analyzed and distributed.

The second most cited article, with 143 citations, was the work by Xu and Nygard (2006), who showed that PrT nets can be an effective approach to formal modeling and verification of attack behaviors, and can capture both control flows and data flows and complex attacks with partially ordered actions.

Jiang et al. (2014) achieved the third largest citation count (99), whose work stated that energy theft is one of the most important concerns related to the smart grid implementation, and presented an attack tree based threat model to illustrate the energy-theft behaviors in Advanced Metering Infrastructure (AMI).

With the same number of citations (90), Torr (2005) focused on planning security activities, and his work stated that we should identify key security objectives together with security feature requirements that are based on customer demand and compliance with standards. Cardenas et al. (2009) provided a holistic view of the security requirements and threat models of the sensor networks focused on high-level security goals. They developed a function to capture the overall effect of various attacks on the high-level security requirements, and to best defend the deployed sensor network.

4.2. *Definition of threat modeling*

We have studied some of the definitions of threat modeling as stated in selected articles in our literature review, as it can answer the research question “what is threat modeling”, and provide us insight into the adoption of threat modeling. The clearest result we found was that the definitions of threat modeling are numerous, and used in many different and perhaps also incompatible ways.

A widely applicable threat modeling definition was given by Uzunov and Fernandez (2014), who stated “threat modeling is a process that can be used to analyze potential attacks or threats, and can also be supported by threat libraries or attack taxonomies”. Similarly, threat modeling “provides a structured way to secure software design, which involves understanding an adversary’s goal in attacking a system based on system’s assets of interest” (Bedi et al., 2013). From the viewpoint of system evaluation, through threat modeling activity, “the architecture of the system is represented and analyzed, potential security threats are identified, and appropriate mitigation techniques are selected” (Dhillon, 2011; Frydman et al., 2014). While focused on application development, “threat modeling is the technique that assists software engineers to identify and document potential security threats associated with a software product, providing development teams a systematic way of discovering strengths and weaknesses in their software applications” (Baquero et al., 2015). It is “a process to analyze the security and vulnerabilities of an application or network services” (Dahbul et al., 2017),

Table 2 – Details of threat modeling publication outlets.

Journal	Ref.
IEEE Security & Privacy	Torr (2005); Dhillon (2011); Steven (2010); Sabbagh and Kowalski (2015)
Computer Networks	Bryant and Saiedian (2017); Meszaros and Buchalcevova (2017)
International Journal of Critical Infrastructure Protection	Burmester et al. (2012); Huang et al. (2009)
International Journal of Safety and Security Engineering	Musman and Turner (2018); Al-Fedaghi and Moein (2014)
Security and Communication Networks	Pan and Zhuang (2017); Li et al. (2014)
Software-Practice & Experience	Li et al. (2009); Marback et al. (2013)

Table 3 – Details of five most cited threat modeling articles.

Ref.	Title	Citations
Deng et al. (2011)	A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements	183
Xu and Nygard (2006)	Threat-driven modeling and verification of secure software using aspect-oriented Petri nets	143
Jiang et al. (2014)	Energy-theft detection issues for advanced metering infrastructure in smart grid	99
Torr (2005)	Demystifying the threat-modeling process	90
Cardenas et al. (2009)	Rethinking security properties, threat models, and the design space in sensor networks: A case study in SCADA systems	90

and provides “a systematic way to identify threats that might compromise security which has been a well-accepted practice by the industry” (Marback et al., 2013).

4.3. *Type of threat modeling methods*

In this subsection, we classify the threat modeling methods, used or proposed by articles from C1 and C2, separately, into “manual/automatic modeling” and “formal/graphical modeling”. This can help us understand state-of-the-art threat modeling methods. “Formal modeling” is a method based on mathematical models, and “graphical modeling” can be attack trees, attack graphs, or tables. The classification results are shown in Tables 4 and 5. Note that ● means the method was addressed in detail, and ◗ means the method was partially addressed (e.g., the method was briefly outlined in a graphical way, but without detailed information). The method types are not mutually exclusive.

From Table 4, it is worth observing that there is a vast majority of articles focusing on manual modeling (27 articles), compared to automatic modeling (4 articles). Moreover, 25 out of 29 articles used graphical descriptions in their threat modeling work.

In automatic modeling, Xu et al. (2012) presented an approach to automated generation of security tests by using formal threat models, but these require manual analysis of the tests that are executed without failure or exception. Besides, Arsac et al. (2011) employed SAT-based model checker SATMC (Armando and Compagna, 2005) to validate the protocols under new threats, so that retaliation and anticipation attacks can be found automatically, but the Multi-Attacker (MA) threat model they proposed remains manual. Baquero et al. (2015) employed Microsoft’s SDL Threat Modeling Tool, which offers automated analysis of security threats of systems, and can be represented by Data Flow Diagrams (DFDs). However, the modeling remains manual. Musman and Turner (2018) employed cyber security game algorithms, which automated several expert level capabilities, such as the combinatorics of possible incidents, attack path discovery, and portfolio analysis, so that analysts do not have do them manually.

Among articles using graphical modeling, Jiang et al. (2014), Hofmann and Kasseckert (2011), and Almulhem (2012) employed attack trees, while Pei et al. (2004) used fault tree. By using tables, Liu et al. (2015) modeled the attack types, targeted information flows, occurring locations and attack techniques in a smart meter. Also, Hofmann and Kasseckert (2011) provided an assessment of potential adversaries and their motivations, as well as their skills and capabilities for attacking telecommunication network equipment (Dahbul et al., 2017). Pendergrass et al. (2014) proposed a threat table approach, which will “absent the need for learning a formal method or needing an automated tool”, and that is “simpler than formal models”. Besides, Bedi et al. (2013) employed STRIDE model (spoofing identity, tampering with data, repudiation, information disclosure, denial of service, and elevation of privilege), and enumerated the asset threatened in a table.

It is also clear to see from Table 4 that, threat modeling methods can be both formal and graphical. For example, Xu and Nygard (2006) and Xu et al. (2012) used PrT nets, which can be both formal and graphical modeling, and the articles focused on the formal part. Also, Yan et al. (2014) adopted a minimum distance threat model, which is both formal and graphical.

Compared with C1 in Table 4, a similar trend can be seen for C2 in Table 5, that 18 out of 20 articles used manual modeling, while only 4 articles used automatic modeling. A model-based tool proposed by Singh et al. (2004) includes both manual and automatic modeling, because the tool was semi-automated, and was constructed with the help from analysts. To reduce the need for costly human expertise to perform risk analysis in software, Frydman et al. (2014) automated the threat identification and mitigation step. Marback et al. (2013) proposed a threat model-based security testing approach, which automatically generates security test sequences from threat trees

Table 4 – Type of threat modeling methods (C1).

Ref.	Manual	Automatic	Formal	Graphical
Xu and Nygard (2006)	●		●	◗
Xu et al. (2012)	◗	●	●	◗
Jiang et al. (2014)	●		◗	●
Yan et al. (2014)	●		●	◗
Pei et al. (2004)	●			●
Liu et al. (2015)	●			●
Hofmann and Kasseckert (2011)	●			●
Cardenas et al. (2009)	●		●	◗
Arsac et al. (2011)	●	◗	●	
Martina et al. (2015)	●		●	
Idziorek and Tannian (2012)	●			●
Paladi et al. (2016)	●		●	
Meszaros and Buchalcevova (2017)	●			●
Wu and Wei (2017)	●		●	◗
Bauer (2013)	●			●
Seifert and Reza (2016)	●			●
Lavrova and Pechenkin (2015)	●			●
Baquero et al. (2015)		●		●
James and Prabakaran (2015)	●			●
Dahbul et al. (2017)	●		●	◗
Chen et al. (2012)	●		●	
Musman and Turner (2018)		●	●	◗
Kalinin and Konoplev (2014)	●		●	◗
Pendergrass et al. (2014)	●			●
Al-Fedaghi and Alkandari (2011)	●			●
Olawumi et al. (2017)	●			●
Almulhem (2012)	●			●
Bedi et al. (2013)	●			●
Dimitriadis (2013)	●			●

Table 5 – Type of threat modeling methods (C2).

Ref.	Manual	Automatic	Formal	Graphical
Singh et al. (2004)	◗	◗	●	◗
Kammüller and Probst (2015)	●		●	
Sabbagh and Kowalski (2015)	●			●
Uzunov and Fernandez (2014)	●		●	◗
Frydman et al. (2014)		●	◗	●
Burmester et al. (2012)	●		●	
Rhee et al. (2013)	●			●
Bryant and Saiedian (2017)	●			●
Deng et al. (2011)	●			●
Sharma et al. (2013)	●		●	●
Marback et al. (2013)	◗	●	●	●
Suleiman et al. (2015)	●			●
Al-Fedaghi and Moein (2014)	●		◗	●
Brændeland et al. (2010)	●		●	●
Pan and Zhuang (2017)	●		◗	●
Lenzini et al. (2015)		●	●	
Magklaras et al. (2006)	●		●	
Huang et al. (2009)	●		●	
Li et al. (2009)	●		●	◗
Li et al. (2014)	●		●	◗

and transforms them into executable tests, however, these test cases had to be executed on multiple computers simultaneously, which involved writing a test harness manually. Besides, Lenzini et al. (2015) defined a formal model for automatic security analysis in socio-technical physical system.

Moreover, many articles employed graphical modeling, and also combined with formal modeling. For test generation, Marback et al. (2013) generated security test sequences from threat trees and proposed a test sequence generation algorithm, which is both graphical and formal. Besides,

Table 6 – System types addressed by articles in C1.

Category		References
General	Software application	Xu and Nygard (2006); Xu et al. (2012); Chen et al. (2012); Al-Fedaghi and Alkandari (2011); Bedi et al. (2013)
	ICT system	Lavrova and Pechenkin (2015); Musman and Turner (2018); Dahbul et al. (2017); Meszaros and Buchalcevova (2017); Pei et al. (2004)
	Smart grid system	Kalinin and Konoplev (2014)
	Cloud computing	Idziorek and Tannian (2012); Paladi et al. (2016)
	Security protocol	Arsac et al. (2011); Martina et al. (2015)
Specific	AMI	Jiang et al. (2014); Liu et al. (2015)
	Vehicular ad hoc network (VANET)	Yan et al. (2014)
	SCADA network	Cardenas et al. (2009); James and Prabakaran (2015)
	CPS architecture for healthcare	Seifert and Reza (2016)
	Software-defined network (SDN)	Wu and Wei (2017)
	Optical cross-connect systems	Hofmann and Kasseckert (2011)
	Network mobility protocol	Bauer (2013)
	Unmanned aerial systems	Baquero et al. (2015)
	Telemedicine application	Pendergrass et al. (2014)
	Smart home environments	Olawumi et al. (2017)
	Electronic Health Record Systems	Almulhem (2012)
	Mobile telecommunication network	Dimitriadis (2013)

Table 7 – System types addressed by articles in C2.

Category		References
General	Software application	Deng et al. (2011); Li et al. (2009); Li et al. (2014); Sabbagh and Kowalski (2015); Bryant and Saiedian (2017)
	ICT system	Frydman et al. (2014); Al-Fedaghi and Moein (2014); Magklaras et al. (2006)
	Cyber human systems	Kammüller and Probst (2015)
	Cyberspace	Sharma et al. (2013); Marback et al. (2013)
	Distributed systems	Uzunov and Fernandez (2014)
	CPS	Burmester et al. (2012)
	Smart grid system	Suleiman et al. (2015)
	Control system	Huang et al. (2009)
Specific	Terrorist network	Singh et al. (2004)
	Mobile device management system	Rhee et al. (2013)
	Power supply system	Brændeland et al. (2010)
	Socio-technical physical system	Lenzini et al. (2015)
	Windows operating system	Pan and Zhuang (2017)

Al-Fedaghi and Moein (2014) employed a graphical flow model of attack progression, and they formally specified the flow model. Brændeland et al. (2010) proposed a risk graph method which can represent fault tree, CORAS threat diagram and assumptions, and also provided formal semantics of the risk graph. Similarly, Pan and Zhuang (2017) proposed a threat model denoted by a tuple, and used an intuitive description of the model. Li et al. (2009) designed a weight distribution algorithm, and used a threat tree to verify its effectiveness, which is both formal and graphical, and the articles focused on the formal part.

4.4. *Systems addressed*

The objective of threat modeling is to prevent, or mitigate the effects of threats and attacks to a system. Therefore, knowing the system and looking for "what can go wrong" are important for threat modeling. In this section, we classify the systems addressed by articles in C1 and C2 into "general/specific system", and the results are shown in Tables 6 and 7, respectively.

From Table 6, we can see that nearly the same number of articles aimed at securing a general system (15) vs. a specific system (14).

To secure general systems, for instance, Xu and Nygard (2006) and Xu et al. (2012) focused on software applications, while Idziorek and Tannian (2012), and Paladi et al. (2016) aimed at securing cloud computing.

For securing AMI, Jiang et al. (2014) dealt with the energy-theft behaviors, while Liu et al. (2015) captured smart meters behavior on potential threats. Moreover, two articles aimed to secure SCADA networks (Cardenas et al., 2009; James and Prabakaran, 2015).

It can be seen from Table 7 that, 15 out of 20 articles in C2 used threat modeling for a general system (15), while only 5 articles addressed a specific system, e.g., Singh et al. (2004) focused on detecting and tracking terrorist activity in terrorist network, while Rhee et al. (2013) aimed at mobile device management system.

Table 8 – Type of threats and attacks (C1).

Category		References
General	Security threats	Xu and Nygard (2006); Seifert and Reza (2016); Lavrova and Pechenkin (2015); Hofmann and Kasseckert (2011); Bedi et al. (2013); Idziorek and Tannian (2012); Cardenas et al. (2009); Meszaros and Buchalcevova (2017)
	STRIDE threats	Xu et al. (2012); Baquero et al. (2015); Chen et al. (2012); Olawumi et al. (2017)
	Cyber attack	James and Prabakaran (2015); Musman and Turner (2018)
	Virus flow	Al-Fedaghi and Alkandari (2011)
Specific	Energy theft	Jiang et al. (2014)
	Spoofed vehicle location	Yan et al. (2014)
	Invalid update messages, Router overload	Pei et al. (2004)
	False data injection attack	Liu et al. (2015)
	Dolev–Yao attacker	Arsac et al. (2011); Martina et al. (2015)
	VM substitution attack	Paladi et al. (2016)
	Threats on SDN controllers	Wu and Wei (2017)
	Attacks on the packet redirection mechanism	Bauer (2013)
	Attacks to honeypots	Dahbul et al. (2017)
	DoS attacks; Malware distribution; Unauthorized access	Kalinin and Konoplev (2014)
	Security threats in telemedicine	Pendergrass et al. (2014)
	Attacks on EHR system	Almulhem (2012)
	Intruder attack on mobile operator	Dimitriadis (2013)

Table 9 – Type of threats and attacks (C2).

Category		References
General	Security threats	Sabbagh and Kowalski (2015); Frydman et al. (2014); Deng et al. (2011); Uzunov and Fernandez (2014); Bryant and Saiedian (2017); Marback et al. (2013); Suleiman et al. (2015); Brændeland et al. (2010); Li et al. (2009); Li et al. (2014); Brændeland et al. (2010); Al-Fedaghi and Moein (2014)
	Cyber attack	Sharma et al. (2013)
Specific	Terrorist threats	Singh et al. (2004)
	Multi-vector attacks	Burmester et al. (2012)
	Attacks on mobile device management system	Rhee et al. (2013)
	Insider attack	Kammüller and Probst (2015); Magklaras et al. (2006)
	Intruder attack	Lenzini et al. (2015)
	Integrity attacks; DoS attacks	Huang et al. (2009)
	Process memory data extraction	Pan and Zhuang (2017)

Common general systems addressed in C1 and C2 are software applications, ICT systems, and smart grids, while there seem to be no common specific systems.

4.5. *Type of threats and attacks*

This section allows us to understand what threats and attacks the threat modeling methods aimed to protect against. We classify the type of threats and attacks for C1 and C2 separately. The results for C1 are shown in Table 8, while for C2 the results are shown in Table 9.

We can see from Table 8 that, nearly the same number of articles in C1 employed threat modeling for a general threat or attack compared to a specific one (15 articles vs. 14 articles). For C2 (cf. Table 9) a large number of articles focused on general security threats.

Regarding the general threats, four articles used STRIDE-based threat modeling, which has been widely used for threat modeling. To be more specific, Xu et al. (2012) presented an approach that automatically generated security tests by using formal threat models represented as PrT nets. Baquero et al. (2015) discussed security issues in aviation and a case study showed a realistic cyber-physical system (CPS) to introduce a STRIDE threats-based threat modeling method. Also, Chen et al. (2012) designed a SN-Security Evaluation Mode according to threat classification method of STRIDE model. Besides, Olawumi et al. (2017) classified possible threats to a system according to the STRIDE taxonomy.

By protecting against a specific attack, Jiang et al. (2014) focused on the energy theft problems of smart grid implementation, while Yan et al. (2014) aimed at spoofed vehicle location attack scenarios. Besides, Wu and Wei (2017) focused on threats on SDN controllers.

From Table 9, we can see that 8 out of 20 articles proposed their threat models based on a specific threat or attack. For example, Singh et al. (2004) focused on detecting and tracking terrorist activity, and Burmester et al. (2012) addressed multi-vector threats, while Rhee et al. (2013) aimed at all possible threats against a mobile device management system. Moreover, Kammüller and Probst (2015) and Magklaras et al. (2006) aimed at insider threats, while Lenzini et al. (2015) focused on intruder attacks.

Another interesting class of articles in C2 focused on general threats and attacks, for example, Frydman et al. (2014) aimed to automate the threat identification and mitigation step based on identification trees and mitigation trees; and Bryant and Saiedian (2017) worked with the practical application of threat modeling of forensic work, while Sharma et al. (2013) focused on cyber attack.

4.6. *Focus and approach*

Studying the focus and approach of the threat modeling articles is important, as it helps us understand what problems were tackled by threat modeling, and how to tackle these issues. The focuses can be classified into "application development", which can be analyzing the security of one or a set of software applications in the design phase, as well as "system evaluation", which takes more than just software into consideration. For C1, we are also interested in their purpose of using threat modeling.

From Table 11 (C1), we observe that 14 out of 29 articles focused on application development, e.g., software design (Xu and Nygard, 2006), smart grid implementation (Jiang et al., 2014), and security needs in healthcare (Seifert and Reza, 2016).

While 15 articles used threat modeling methods for system evaluation, for example, to secure a specific system or to analyze a protocol. To be more specific, three articles used Dolev–Yao's threat model (Arsac et al., 2011; Martina et al., 2015; Paladi et al., 2016), four articles used attack or fault trees (Jiang et al., 2014; Pei, et al., 2004; Almulhem, 2012; Dimitriadis, 2013), four articles employed PrT or Petri nets (Xu and Nygard, 2006; Xu, et al., 2012; Liu et al., 2015; Kalinin and Konoplev, 2014), and three articles used the STRIDE model (Seifert and Reza, 2016; Chen et al., 2012; Pendergrass et al., 2014); two articles used DFD (Al-Fedaghi and Alkandari, 2011; Olawumi et al., 2017).

From Table 12 (C2), we can infer that 8 out of 20 articles focused on application development. For example, Sabbagh and Kowalski (2015) employed security-by-consensus (SBC) model, and established a socio-technical framework to secure software supply chain. Bryant and Saiedian (2017) presented a kill-chain model with specific phases designed to facilitate metadata aggregation.

While focused on system evaluation, for instance, Singh et al. (2004) used hidden Markov models (HMMs) and Bayesian networks (BNs) to analyze the threat level of potential terrorist attacks. Kammüller and Probst (2015) combined formal modeling and analysis of infrastructures of organizations with sociological explanation, to provide a framework for insider threat analysis. Burmester et al. (2012) proposed a framework for modeling the security of a CPS based on Byzantine paradigm, and can support formal analyses and security proofs of CPSs.

As different knowledge bases can help to identify and analyze threats, many articles were supported by external sources. However, related quantitative threat modeling techniques were only sparsely used in these articles (12 out of 29 in C1; 7 out of 20 in C2).

For C1, we also study the purpose of using threat modeling. To be more specific, Xu and Nygard (2006) used threat modeling to explore explicit behaviors of security threats, and also to automated generation of security tests (Xu et al., 2012). Besides, Cardenas et al. (2009) used threat modeling to formalize the perceived risk, defend against threats to application layer, and Lavrova and Pechenkin (2015) employed threat modeling to describe an adaptive deceptive system and policies of reflexive control.

4.7. *Methods of validation*

This subsection aims to identify the type of validation methods used in the articles. Analysis techniques that explicitly assure the outcomes for quality define this activity as part of the analysis procedure. For instance, if the outcomes are represented with models, the technique may perform model verification as part of the analysis procedure. Note that the validation methods are not mutually exclusive.

As is shown in Table 10, the majority of articles were validated through theoretical examples or empirical case studies (a research methodology used to study a real phenomenon of exploratory, descriptive, explanatory and improving purpose).

Nearly 50% of the articles used empirical validation methods (if we include implementation in this category). Also, there was no validation performed in 4 out of 29 articles in C1.

Also, examples and case studies were mostly used to validate threat models in C2 (cf. Table 13). Some of them used qualitative methods (Burmester et al., 2012; Kammüller and Probst, 2015), and Singh et al. (2004) used software simulations on the likelihood of observations, as well as the probability of a terrorist attack. Still, 3 out of 20 articles in C2 proposed their threat models without any validation.

4.8. *Threat modeling process articles (C3)*

Cluster 3, so far not presented in this section, includes introductory articles focused on e.g., the threat modeling process. To be more specific, Torr (2005) stated that "the threat-model document's heart, and the most useful tool for generating threats against the component is the DFD, which is a graphical representation of the component, and shows all the inputs and outputs as well as all logical internal processes". Also employed DFD, Dhillon (2011) collected information about target industry systems, and formed relevant representations.

Besides, Steven (2010) stated that "the threat-modeling steps can not only uncover missing or broken security controls, but also uncover where non-security elements of an application's design might profoundly affect its security posture any service/software". Kamatchi and Ambekar (2016) stated that "threat modeling is an iterative process, because identifying threats at one attempt is almost impossible, and applications/services are no more static and there are tremendous changes in business processes which need to be thought about while creating them".

In order to reduce information risks in libraries with comprehensive information resources, Rodionova and Bobrov (2016) emphasized that "the basic document for information

Table 10 – Validation methods (C1).

Category		References
Theoretical	Simulation	Yan et al. (2014); Liu et al. (2015); James and Prabakaran (2015)
	Analysis	Cardenas et al. (2009); Arsac et al. (2011); Wu and Wei (2017); Bauer (2013); Al-Fedaghi and Alkandari (2011); Almulhem (2012)
	Example	Seifert and Reza (2016); Lavrova and Pechenkin (2015); Musman and Turner (2018); Kalinin and Konoplev (2014); Olawumi et al. (2017); Dimitriadis (2013)
Empirical	Case study	Xu and Nygard (2006); Xu et al. (2012); Meszaros and Buchalcevova (2017); Baquero et al. (2015); Chen et al. (2012); Pendergrass et al. (2014); Bedi et al. (2013)
	Implementation	Martina et al. (2015); Paladi et al. (2016); Dahbul et al. (2017)
	Expert review	Dahbul et al. (2017)
Not specified		Jiang et al. (2014); Pei et al. (2004); Hofmann and Kasseckert (2011); Idziorek and Tannian (2012)

security risk management is a threat model that reflects the data on sources of threats and vulnerabilities of the system, impacted objects, and a number of other parameters". They also used a block diagram to illustrate the process of analyzing the threats and vulnerabilities.

5. Discussion

5.1. *Limitations of this work*

While this literature review aims to include a large amount and diverse sources, it is time consuming and difficult to review all the literature. We decided to search for journal publications in four leading scientific databases, as the quality of journal articles in these four databases can be ensured. There is a large amount of papers in conference and workshop proceedings that could add some value to this literature review, however we believe that the quality of these are in general more difficult to ensure, and that many might have been further developed into journal publications. We therefore consider that the articles reviewed in this study provide a good general high-quality knowledge base of threat modeling today.

With the focus on threat modeling as a concept, we do miss out on some articles that perhaps doing threat modeling, while not calling it by the name, e.g., attack/defense trees, attack graphs, and graphical modeling for security. However, if we included side concepts, we would bias our results in presenting what threat modeling is today. We believe that our strict approach sticking to only threat modeling as a keyword gives us more non-biased results.

5.2. *Findings*

In this systematic literature review on threat modeling, the selected 54 articles were classified into three clusters - applying threat modeling (C1), threat modeling methods (C2), and threat modeling processes (C3). In general, the trend of the articles per year is positive since 2008. Besides, the threat modeling research is attracting worldwide attention, with the largest portion being executed in North America.

To answer the research question "what is threat modeling", the clearest result found was that threat modeling is a diverse field lacking common ground. The definitions are numerous, and used in many different and perhaps also incompatible ways. Despite this, a widely accepted one seems to be "threat modeling is a process that can be used to analyze potential attacks or threats, and can also be supported by threat libraries or attack taxonomies" (Uzunov and Fernandez, 2014).

To answer the research question "what is the state-of-the-art work in this field", in terms of the threat modeling methods, we found that articles from both C1 and C2 focused more on manual modeling than automatic modeling. It symbolizes that most threat modeling work remains to be done manually, which can be time-consuming and error-prone (Närman et al., 2009; Holm et al., 2014). Thus, the trend is to model a system with a higher degree of automation, e.g., automate the security analysis. Also, some articles combined both of manual and automatic modeling (e.g., Xu et al., 2012), and some articles employed both graphical and formal modeling methods (e.g., Brændeland et al., 2010), with various weights. It reflects that the form of threat modeling can be flexible. In terms of the system they are aiming to protect, software applications, ICT systems and smart grids were commonly addressed (all being at a fairly general level), while there seem to be no common more specific systems addressed in the reviewed articles. Besides, to understand what threats and attacks these articles aimed to protect against, we found that, the largest portion is general security threats, while other (but fewer) focused on various specific threats and attacks. Moreover, to understand what problems that were tackled by threat modeling and how to tackle them, we found that they either focused on application development (e.g., software design) or system evaluation (e.g., more holistic system-wide analysis). Also, many articles were supported by external sources (e.g., Dolev–Yao's threat model). However, quantitative techniques were barely used. We believe that there is room and a need for more development and employment of quantitative methods. Furthermore, the validation methods can be generally classified into theoretical ones (e.g., simulation) and empirical ones (e.g., case studies), while we observe that there is limited assurance of these validation methods.

5.3. *Future research directions*

Future research directions mentioned in the reviewed articles can be classified into the following categories:

Design automatic threat modeling method: Huang et al. (2009) described an approach for developing threat models for

Table 11 – Focus and approach (C1).

Ref.	Focus		Approach			
	Application	System	Presenting a new	Using an existing	Qualitative	Quantitative
Xu and Nygard (2006)	Software design		Formal threat-driven approach	Aspect-oriented PrT nets	Threat and mitigation verification	
Xu et al. (2012)	Software testing			PrT nets	Generate all attack paths and convert them into executable code	
Jiang et al. (2014)	Smart grid implementation			Attack tree	Support Vector Machine for energy-theft detection	Minimize classification error
Yan et al. (2014)	Form an optimal decision rule on the legitimacy of the claimed location		Information-theoretic framework on location verification system (LVS)			Simulate the normalized mutual information (NMI) under the MD threat model
Pei et al. (2004)		Enhance the resiliency of the network routing protocols component		Fault tree	Use fault tree to represent threats in routing	
Liu et al. (2015)	Smart meters security		Collaborative intrusion mechanism	Colored Petri net		Category attack techniques
Hofmann and Kasseckert (2011)		Form a security architecture for transmission systems		Functional reference models	List a table of adversaries and their motivations	
Cardenas et al. (2009)	Sensor network security for practical deployments		A taxonomy composed of the security properties			Security metrics
Arsac et al. (2011)		Validate protocols under threats	Multi-Attacker threat model	Dolev–Yao's threat model	Analysis of a classical protocol under threat model	
Martina et al. (2015)		Security ceremonies		Dolev–Yao's threat model	Theorem analysis	
Idziorek and Tannian (2012)	Cloud-hosted application		Analysis of the security aspects of the cloud model	Parker's six security elements		
Paladi et al. (2016)		Public infrastructure clouds	Domain-based storage protection (DBSP)	Dolev–Yao's threat model		
Meszaros and Buchalcevova (2017)	Online services security risk management		Online Services Security Framework	OWASP Risk Rating Methodology	Threat classification	Possible risk severity levels and risk scores
Wu and Wei (2017)		Secure SDN	Threat/Effort Model (TE model)			TE Value
Bauer (2013)		Secure correspondent router protocol	Network mobility route optimization procedure			Handover delay
Seifert and Reza (2016)	Security needs of CPS in healthcare			STRIDE threat model, DREAD risk ranking	Threat classification	Risk ranking

(*continued on next page*)

Table 11 (*continued*)

Ref.	Focus		Approach			
	Application	System	Presenting a new	Using an existing	Qualitative	Quantitative
Lavrova and Pechenkin (2015)		Increase the degree of information security	Concept of an adaptive deceptive system		Divide threats into four classes according to the layer	
Baquero et al. (2015)	Unmanned aerial systems security analyses			Microsoft SDL	Build DFD, security risk assessment	
James and Prabakaran (2015)		Identify cyber vulnerabilities in SCADA systems		OMNeT tool	Identification of cyber vulnerabilities; Criticality assessment	
Dahbul et al. (2017)		Identify potential threats which made honeypot ineffective		Honeypot systems	Enumerate all possible security threats	Time-to-live data
Chen et al. (2012)	Evaluate the degree of software security		SN-Security Evaluation Model	STRIDE model		Evaluate security degree
Musman and Turner (2018)		Minimize cybersecurity risks	Cyber Security Game	Game theory		Risk score
Kalinin and Konoplev (2014)		Secure grid systems resources		Petri nets	Integrate Petri net into grid system	
Pendergrass et al. (2014)	Security threats to telemedicine application		Threat table approach	STRIDE model	List conceptual tasks	
Al-Fedaghi and Alkandari (2011)	Develop secure software		Flow-based methodology	DFD; SDL	Provide a conceptual specification	
Olawumi et al. (2017)		Secure smart home environments	Smart Environment for Assisted Living (SEAL)	DFD		Evaluate possibility of risks
Almulhem (2012)		Analyze threats facing EHR systems		Attack tree	Augment an attack tree	
Bedi et al. (2013)		Proactive risk management	Three-phased threat-oriented security model	Microsoft's Threat Modeling Tool		
Dimitriadis (2013)	Security assessments of major mobile operators			Combined attack tree	Vulnerability groups, identify possible attacks	

Table 12 – Focus and approach (C2).

Ref.	Focus		Approach			
	Application	System	Presenting a new	Using an existing	Qualitative	Quantitative
Singh et al. (2004)		Predict a terrorist event		Hidden Markov models; Bayesian networks		Prior probability of threats
Kammüller and Probst (2015)		Provide a framework for insider threat analysis	Isabelle/Higher order logic model	Weber's social explanation	Logical analysis of insider threats	
Sabbagh and Kowalski (2015)	Establish a secure software supply chain			Security-by-consensus (SBC) model	Gather professional opinions on threats	
Uzunov and Fernandez (2014)	Software engineering		Two-level pattern-based threat taxonomy	Threat libraries; Threat taxonomies	Encompass threats to a system and threats to realizations	
Frydman et al. (2014)	Software design		Automated security expert consultant (AutSEC)	DFD	4-step process to generate three detailed reports	Risk ranking
Burmester et al. (2012)		Protect cyber-physical features		Byzantine model	Use threat transition to model CPS vulnerabilities	
Rhee et al. (2013)		Secure a mobile device management system	Threat modeling methodology		Threat-Attack-Asset-Effect	
Bryant and Saiedian (2017)	Software design		Bryant Kill-Chain	Kill-chain model		Detection rate
Deng et al. (2011)	Elicit privacy requirements, and instantiate privacy-enhancing countermeasures		LINDDUN framework	DFD; Threat tree	Map threat types with elements in the system model	
Sharma et al. (2013)		Secure cyberspace		Combination of Formal Concept Analysis and hierarchical fact-proposition space inference	Formal concept analysis	Belief value
Marback et al. (2013)	Software testing		A threat model-based security testing approach	STRIDE model; Threat tree	Generates security test sequences and transforms into executable tests	
Suleiman et al. (2015)		Depict and understand vulnerabilities in smart grid	Smart Grid Systems Security Threat Model (SG SSTM)		Classify threats into 5 categories	
Al-Fedaghi and Moein (2014)		Model computer and communication system threat risks		Flow model	Conceptual describe attack	
Brændeland et al. (2010)		Deduce risk level of power supply system	Risk graph		Represent risk modeling techniques in risk graph	

(continued on next page)

Table 12 (*continued*)

Ref.	Focus		Approach			
	Application	System	Presenting a new	Using an existing	Qualitative	Quantitative
Pan and Zhuang (2017)		Secure process memory data	Process Memory Captor		Formula description of threat model	Model threat value
Lenzini et al. (2015)		Secure socio-technical physical systems				
Magklaras et al. (2006)		Mitigating insider threats in IT environments	A language to abstract insider threat	Common intrusion specification language (CISL)	Abstract information into language semantics	
Huang et al. (2009)		Secure control systems	Control system abstraction		Formally model integrity and DoS attacks	
Li et al. (2009)	Secure software		Attack path evaluating algorithm	Threat tree		Threat coefficients
Li et al. (2014)	Improve the trustworthiness of software designs		Unified threat model		Present software threats unified threat model	Attack path search algorithm; Software threat evaluation algorithm

Table 13 – Validation methods (C2).

Category		References
Theoretical	Simulation	Singh et al. (2004); Huang et al. (2009)
	Analysis	Suleiman et al. (2015); Lenzini et al. (2015)
	Example	Burmester et al. (2012); Al-Fedaghi and Moein (2014); Li et al. (2009); Uzunov and Fernandez (2014)
Empirical	Case study	Kammüller and Probst (2015); Sabbagh and Kowalski (2015); Frydman et al. (2014); Deng et al. (2011); Brændeland et al. (2010); Pan and Zhuang (2017); Lenzini et al. (2015); Li et al. (2014)
	Application	Bryant and Saiedian (2017); Marback et al. (2013)
	Interview	Sabbagh and Kowalski (2015)
Not specified		Rhee et al. (2013); Sharma et al. (2013); Magklaras et al. (2006)

attacks on control systems, and stated that future research should focus on designing automatic attack detection and response mechanisms that can enhance the resilience of control systems. Similarly, Li et al. (2009) said that important future work is to design automatic attack detection and response mechanisms that can enhance the resilience of control systems.

Validation of threat modeling: Further research directions proposed by Singh et al. (2004) includes validating how usable the approach is for intelligence analysts. Also, Deng et al. (2011) planned to apply a threat analysis framework in larger case studies. Brændeland et al. (2010) proposed a modular approach to the modeling and analysis of risk scenarios with dependencies, and future work might combine the approach with high-level diagrams that describe threat scenarios at a higher abstraction level. Al-Fedaghi and Moein (2014) suggested also experimenting with modeling of real environments such as describing actual computer attacks. Marback et al. (2013) intended to apply their approach to more applications and perform controlled experiments for evaluating. Hofmann and Kasseckert (2011) developed a profile for a "powerful" attacker against whom such equipment should be protected, next steps would include verifying the concept of security zones and defining a respective security architecture, and then be analyzed regarding its security characteristics and its applicability in real systems. Cardenas et al. (2009) stated that the analysis of their threat model may not be a definitive solution to the problem of threat modeling in sensor networks, and future research directions would address the problem in a more systematic way.

Implement threat modeling as a software tool: Lenzini et al. (2015) defined a framework for automatic security analysis of socio-technical physical systems, and they plan to implement their framework as a software tool that fully supports all steps in the design and analysis of socio-technical physical systems. Future work of Bedi et al. (2013) includes making threat-oriented security framework a cost-oriented and economically viable security solution, to give a new dimension to risk management.

Integrate defenses into threat modeling: Pan and Zhuang (2017) suggested more defenses should be integrated into threat modeling.

Derive new attack categories: Sharma et al. (2013) identified attack factors and attributes in social dimension, their suggestion for future work is deriving new attack categories. Meszaros and Buchalcevova (2017) derived that their framework must be continuously updated in the future, because new kinds of threats and vulnerabilities would arise along with evolution of technologies.

5.4. *Our future work*

Our future work includes proposing an automatic threat modeling method, building on the Meta Attack Language (MAL) (Johnson et al., 2018). And validate it with test cases (similar to Xiong et al., 2019) and real-world case studies (similar to Lagerström et al., 2010, 2013). Also, we will focus on specific domains where threat modeling is absent or still immature. For example, to improve the security for connected vehicles, and proactively design for security, we will enhance the threat models with probabilistic attack simulations (Johnson et al., 2016). Thus, we will research more in vehicle-specific attacks and countermeasures to provide more accurate simulation results, e.g. through machine learning techniques (Lagerström et al., 2017) on predicting threat probabilities. Besides, we will propose a more tailored metamodel for connected vehicles, as most threat modeling metamodels today are created for office IT or similar systems, which only reflect parts of a system (extending Katsikeas et al., 2019). We will also consider the data privacy aspect, as large amounts of data today are generated and communicated in vehicular networks, and are more or less sensitive for the drivers of the vehicles. We aim to improve the privacy of connected vehicles through privacy mechanisms like differential privacy.

6. Conclusion

Cyber security is a critical aspect of networks, computers, software, and data, and therefore attracting worldwide attention. As a significant part of cyber security, threat modeling is becoming widespread in both application development and system evaluation. Unfortunately, it is a domain that lacks common ground. To understand what threat modeling is, and what the state-of-the-art work in this field is, we conducted a systematic literature review on threat modeling. To the best of our knowledge, this is the first SLR on this topic. Following a strict and transparent review methodology, 176 articles were assessed from four leading scientific databases, and 54 of them were selected for further analysis.

The main findings are that, threat modeling is a diverse field lacking common ground, and the definitions are numerous and used in many different ways. Also, the threat modeling work remains to be done manually, which can be time-consuming and error-prone. Moreover, the form of threat modeling is flexible (graphical, formal, qualitative, quantitative), sometimes with a focus on being general and other times more specific (both in terms of threats and application domain), and validation methods are of varied types.

Based on the findings, future research directions are given. Firstly, the research trend is to model a system with a higher degree of automation, e.g., automate the security analysis and/or the modeling. Also, validation methods need to be developed and enhanced for assuring the outcomes of threat modeling (less examples and more empirics). Besides, integration with threat and vulnerability databases would be a natural next step, and more (better) commercial threat modeling tools could be offered. Both researchers and practitioners can benefit from our study getting a better understanding of the state-of-the-art threat modeling methods out there. Our own future work includes threat modeling for connected vehicles, to improve security and privacy.

Conflict of interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

This work has received funding from the Swedish Governmental Agency for Innovation Systems (Grant agreement number: 2017-03087) and its program on Strategic Vehicle Research and Innovation as well as the STandUp for Energy program.

Supplementary materials

Supplementary material associated with this article can be found, in the online version, at doi:10.1016/j.cose.2019.03.010.

REFERENCES

Al-Fedaghi S, Alkandari A. On security development lifecycle: conceptual description of vulnerabilities, risks, and threats. Int J Digital Content Technol Appl 2011;5(5):296–306.

Al-Fedaghi S, Moein S. Modeling attacks. Int J Saf Secur Eng 2014;4(2):97–115.

Alharbi S, Weber-Jahnke J, Traore I. The proactive and reactive digital forensics investigation process: a systematic literature review. Information Security and Assurance. ISA 2011. Communications in Computer and Information Science, 200. Berlin, Heidelberg: Springer; 2011. p. 87–100.

Almulhem A. Threat modeling for electronic health record systems. J Med Syst 2012;36(5):2921–6.

Armando A, Compagna L. An optimized intruder model for SAT-based model-checking of security protocols. Electron Notes Theor Comput Sci 2005;125(1):91–108.

Arsac W, Bella G, Chantry X, Compagna L. Multi-Attacker Protocol Validation. J Automat Reason 2011;46(3-4):353–88.

Baquero AO, Kornecki AJ, Zalewski J. Threat modeling for aviation computer security. CrossTalk 2015;28:21–7.

Basin D, Cremers C, Miyazaki K, Radomirovic S, Watanabe D. Improving the security of cryptographic protocol standards. IEEE Secur Priv 2015;13(3):24–31.

Bauer C. A secure correspondent router protocol for NEMO route optimization. Comput Netw 2013;57(5):1078–100.

Bedi P, Gandotra V, Singhal A, Narang H, Sharma S. Threat-oriented security framework in risk management using multiagent system. Softw Pract Exp 2013;43: 1013–1038.

Booth AA, Papaioannou D, Sutton A. Systematic approaches to a successful literature review. Los Angeles: SAGE; 2012.

Brændeland G, Refsdal A, Stølen K. Modular analysis and modelling of risk scenarios with dependencies. J Syst Softw 2010;83(10):1995–2013.

Bryant BD, Saiedian H. A novel kill-chain framework for remote security log analysis with SIEM software. Comput Secur 2017;67:198–210.

Burmester M, Magkos E, Chrissikopoulos V. Modeling security in cyber-physical systems. Int J Crit Infrastruct Prot 2012;5(3-4):118–26.

Cardenas AA, Roosta T, Sastry S. Rethinking security properties, threat models, and the design space in sensor networks: a case study in SCADA systems. Ad Hoc Netw 2009;7(8): 1434–1447.

Chen X, Liu Y, Yi J. A security evaluation framework based on STRIDE model for software in networks. Int J Adv Comput Technol 2012;4(13):269–78.

Cucurull J, Asplund M, Nadjm-Tehrani S, Santoro T. Surviving attacks in challenged networks. IEEE Trans Dependable Secure Comput 2012;9(6):917–29.

Dahbul RN, Lim C, Purnama J. Enhancing honeypot deception capability through network service fingerprinting. J Phys Conf Ser 2017;801:1–6.

Deng M, Wuyts K, Scandariato R, Preneel B, Joosen W. A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements. Requir Eng 2011;16(1):3–32.

Dhillon D. Developer-driven threat modeling: lessons learned in the trenches. IEEE Secur Priv 2011;9(4):41–7.

Dimitriadis CK. Security for mobile operators in practice. Int J Netw Secur 2013;15(5):397–404.

Do Q, Martini B, Choo K-KR. A data exfiltration and remote exploitation attack on consumer 3D printers. IEEE Trans Inf Forensics Secur 2016;11(10):2174–86.

Fernández-Alemán JL, Señor IC, Lozoya PÁ, Toval A. Security and privacy in electronic health records: a systematic literature review. J Biomed Inf 2013;46(3):541–62.

Franke U, Brynielsson J. Cyber situational awareness – a systematic review of the literature. Comput Secur 2014;46:18–31.

Frydman M, Ruiz G, Heymann E, César E, Miller BP. Automating risk analysis of software design models. Sci World J 2014;2014:1–12.

Hofmann S, Kasseckert R. Towards a security architecture for IP-based optical transmission systems. Bell Labs Tech J 2011;1(16):133–53.

Holm H, Buschle M, Lagerström R, Ekstedt M. Automatic data collection for enterprise architecture models. Softw Syst Model 2014;13(2):825–41.

Huang Y-L, Cárdenas AA, Amin S, Lin Z-S, Tsai H-Y, Sastry S. Understanding the physical and economic consequences of attacks on control systems. Int J Crit Infrastruct Prot 2009;2(3):73–83.

Hydara I, Sultan AB, Zulzalil H, Admodisastro N. Current state of research on cross-site scripting (XSS) – a systematic literature review. Inf Softw Technol 2015;58:170–86.

Idziorek J, Tannian M. Security analysis of public cloud computing. Intl J Commun Netw Distrib Syst 2012;9(1/2):4–20.

James KI, Prabakaran R. Threat modeling framework for electrical distribution scada networks. Middle-East J Sci Res 2015;9(23):2318–25.

Jiang R, Lu R, Wang Y, Luo J, Shen C, Shen XS. Energy-theft detection issues for advanced metering infrastructure in smart grid. Tsinghua Sci Technol 2014;19(2):105–20.

Johnson P, Lagerström R, Ekstedt M. A meta language for threat modeling and attack simulations. In: Proceedings of the 13th international conference on availability, reliability and security. ACM; 2018. p. 1–8.

Johnson P, Vernotte A, Gorton D, Ekstedt M, Lagerström R. Quantitative information security risk estimation using probabilistic attack graphs. International Workshop on risk assessment and risk-driven testing. Springer; 2016. p. 37–52.

Kalinin M, Konoplev A. Formalization of objectives of grid systems resources protection against unauthorized access. Nonlinear Phenom Complex Syst 2014;17(3):272–7.

Kamatchi R, Ambekar K. Analyzing impacts of cloud computing threats in attack based classification models. Indian J Sci Technol 2016;9(21):1–7.

Kammüller F, Probst CW. Modeling and verification of insider threats using logical analysis. IEEE Syst J 2015;11(2):534–45.

Katsikeas S, Johnson P, Hacks S, Lagerström R. Probabilistic modeling and simulation of vehicular cyber attacks: an application of the meta attack language. In: Proceedings of the 5th international conference on information systems security and privacy (ICISSP); 2019. p. 1–8 *Feb*.

Kitchenham B. Guidelines for performing systematic literature reviews in software engineering. Keele; 2007. EBSE Technical Report EBSE-2007-01.

Lagerström R, Baldwin C, Maccormack A, Dreyfus D. Visualizing and measuring enterprise architecture: an exploratory BioPharma case. In: Proceedings of the 6th IFIP WG 8.1 working conference on the practice of enterprise modeling (PoEM); 2013. p. 9–23.

Lagerström R, Johnson P, Ekstedt M. Architecture analysis of enterprise systems modifiability: a metamodel for software change cost estimation. Softw Qual J 2010;18(4):437–68.

Lagerström R, Johnson P, Ekstedt M. Automatic design of secure enterprise architecture: work in progress paper. In: Proceedings of the trends in enterprise architecture research (TEAR) workshop, in conjunction with the IEEE EDOC conference; 2017. p. 65–70.

Latif R, Abbas H, Assar S, Ali Q. Cloud Computing risk assessment: a systematic literature review. Future information technology. Lecture Notes in Electrical Engineering, 276. Berlin, Heidelberg: Springer; 2014. p. 285–95.

Lavrova DS, Pechenkin AI. Adaptive reflexivity threat protection. Autom Control Comput Sci 2015;49(8):727–34.

Lebek B, Uffen J, Breitner MH, Neumann M, Hohler B. Employees' information security awareness and behavior: a literature review. In: Proceedings of the 46th Hawaii international conference on system sciences (HICSS); 2013. p. 2978–87.

Lenzini G, Mauw S, Ouchani S. Security analysis of socio-technical physical systems. Comput Electr Eng 2015;47:258–74.

Li X, He K, Feng Z, Xu G. Unified threat model for analyzing and evaluating software threats. Secur Commun Netw 2014;7(10):1454–66.

Li X, Liu R, Feng Z, He K. Threat modeling-oriented attack path evaluating algorithm. Trans Tianjin Univ 2009;15(3):162–7.

Liu X, Zhu P, Zhang Y, Chen K. A collaborative intrusion detection mechanism against false data injection attack in advanced metering infrastructure. IEEE Trans Smart Grid 2015;6(5):2435–43.

Magklaras G, Furnell S, Brooke P. Towards an insider threat prediction specification language. Inf Manag Comput Secur 2006;14(4):361–81.

Marback A, Do H, He K, Kondamarri S, Xu D. A threat model-based approach to security testing. Softw Pract Exp 2013;43(2):241–58.

Martina JE, Santos Ed, Carlos MC, Price G, Custódio RF. An adaptive threat model for security ceremonies. Int J Inf Secur 2015;14(2):103–21.

Mellado D, Blanco C, ESánchez L, Fernández-Medina E. A systematic review of security requirements engineering. Comput Stand Interfaces 2010;32(4):153–65.

Meszaros J, Buchalcevova A. Introducing OSSF: a framework for online service cybersecurity risk management. Comput Secur 2017;65:300–13.

Musman S, Turner A. A game oriented approach to minimizing cybersecurity risk. Int J Saf Secur Eng 2018;8(2):212–22.

Närman P, Johnson P, Lagerström R, Franke U, Ekstedt M. Data collection prioritization for system quality analysis. Electron Notes Theor Comput Sci 2009;233:29–42.

Okoli, C., & Schabram, K. (2011). A guide to conducting a systematic literature review of information systems research. Working Papers on Information Systems, 1–49.

Olawumi O, Väänänen A, Haataja K, Toivanen P. Security Issues in smart homes and mobile health system: threat analysis, possible countermeasures and lessons learned. Int J Inf Technol Secur 2017;9(1):31–52.

Paladi N, Gehrmann C, Michalas A. Providing user security guarantees in public infrastructure clouds. IEEE Trans Cloud Comput 2016;5(3):405–19.

Pan J, Zhuang Y. PMCAP: a threat model of process memory data on the windows operating system. Secur Commun Netw 2017;2017:1–15.

Park K, Woo S, Moon D, Choi H. Secure Cyber deception architecture and decoy injection to mitigate the insider threat. Symmetry Secure Cyber World 2018;10(1):1–16.

Pei D, Zhang L, Massey D. A framework for resilient internet routing protocols. IEEE Netw 2004;18(2):5–12.

Pendergrass JC, Heart K, Ranganathan C, Venkatakrishnan VN. A threat table based assessment of information security in telemedicine. Int J Healthc Inf Syst Inf 2014;9(4):20–31.

Rhee K, Won D, Jang S-W, Chae S, Park S. Threat modeling of a mobile device management system for secure smart work. Electron Commer Res 2013;13(3):243–56.

Rodionova ZV, Bobrov LK. Protection of the information resources of a library based on analysis of business processes. Sci Tech Inf Process 2016;43(1):20–7.

Sabbagh BA, Kowalski S. A Socio-technical Framework for threat modeling a software supply chain. IEEE Secur Priv 2015;13(4):30–9.

Seifert D, Reza H. A security analysis of cyber-physical systems architecture for healthcare. Computers 2016;5(27):1–24.

Sharma A, Gandhi R, Zhu Q, Mahoney WR, Sousan W. A social dimensional cyber threat model with formal concept analysis and fact-proposition inference. Int J Inf Comput Secur 2013;5(4):301–33.

Shin M, Cornelius C, Peebles D, Kapadia A, Kotz DK, Triandopoulos N. AnonySense: a system for anonymous opportunistic sensing. Pervasive Mob Comput 2011;7(1): 16–30.

Shuaibu BM, Norwawi NM, Selamat MH, Al-Alwani A. Systematic review of web application security development model. Artif Intell Rev 2015;43(2):259–76.

Singh S, Tu H, Allanach J, Areta J, Willett P, Pattipati K. Modeling threats. IEEE Potentials 2004;23(3):18–21.

Sommestad T, Hallberg J, Lundholm K, Bengtsson J. Variables influencing information security policy compliance: a systematic review of quantitative studies. Inf Manag Comput Secur 2014;22(1):42–75.

Soomro ZA, Shah MH, Ahmed J. Information security management needs more holistic approach: a literature review. Int J Inf Manage 2016;36(2):215–25.

Steven J. Threat modeling – perhaps it's time. IEEE Secur Priv 2010;8(3):83–6.

Suleiman H, Israa Alqassem, Diabat A, Arnautovic E, Svetinovic D. Integrated smart grid systems security threat model. Inf Syst 2015;53(10-11):147–60.

Torr P. Demystifying the threat-modeling process. IEEE Secur Priv 2005;3(5):66–70.

Uzunov AV, Fernandez EB. An extensible pattern-based library and taxonomy of security threats for distributed systems. Comput Stand Interfaces 2014;36(4):734–47.

Wu Z, Wei Q. Quantitative analysis of the security of software-defined network controller using threat/effort model. Math Probl Eng 2017;2017:1–11.

Xiong W, Krantz F, Lagerström R. Threat modeling and attack simulations of connected vehicles: a research outlook. *Proceedings of the 5th international conference on information systems security and privacy (ICISSP)*, 2019.

Xu D, Nygard KE. Threat-driven modeling and verification of secure software using aspect-oriented petri nets. IEEE Trans Softw Eng 2006;32(4):265–78.

Xu D, Tu M, Sanford M, Thomas L, Woodraska D, Xu W. Automated security test generation with formal threat models. IEEE Trans Dependable Secure Comput 2012;9(4):526–40.

Yan S, Malaney R, Nevat I, Peters GW. Optimal information-theoretic wireless location verification. IEEE Trans Veh Technol 2014;63(7):3410–22.

Zawoad S, Dutta AK, Hasan R. Towards building forensics enabled cloud through secure logging-as-a-service. IEEE Trans Dependable Secure Comput 2016;13(2):148–62.

Zhu Y, Fu X, Graham B, Bettati R, Zhao W. Correlation-based traffic analysis attacks on anonymity networks. IEEE Trans Parallel Distrib Syst 2010;21(7):954–67.

Wenjun Xiong is currently a PhD student at KTH Royal Institute of Technology. She obtained her MSc from Wuhan University in 2017. Her current research interests include Threat Modeling, Attack Simulations, and Cyber Security.

Robert Lagerström is an associate professor at KTH Royal Institute of Technology, Stockholm Sweden. Robert's topics of interest include Threat Modeling, Attack Simulations, Software Applications Complexity, and Cyber Security. He teaches on bachelor, master, and PhD level. Robert has written more than 90 academic publications (journals, conferences, and workshops). He is one of the founders and board members of the KTH spin-off company Foreseeti, where he also works as an expert. Foreseeti develops and sells an "IT CAD Tool" for proactive cyber security management called Securicad.