Structured Information Retrieval of Security Ontologies

Malina Adach ✉[0000−0002−7986−2214], Kaj Hänninen[0000−0003−0757−822X], and Kristina Lundqvist[0000−0003−0904−3712]

School of Innovation, Design and Engineering, Mälardalen University, Västerås, Sweden
{malina.adach, kaj.hanninen, kristina.lundqvist}@mdh.se

Abstract. Security ontologies have been created to facilitate the organization and management of knowledge in the security domain. It is a challenge to compare and evaluate how these ontologies relate to one another due to their size, structure, level of expressiveness, and complexity. Ontologies differ in both language and ontological levels, which present obstacles that can lead to errors and inconsistencies in comparisons and alignment attempts. Furthermore, many concepts associated with existing security ontologies have not been fully expounded upon and do not fully comply with security standards. The standards ensure a common understanding of concepts and definitions.

In this study, we address these deficiencies by performing a systematic literature review of existing security ontologies to identify core concepts and relationships. The main goal of the systematic literature review is to identify core concepts and relationships that are used to capture security issues. These concepts and relationships are further analyzed and mapped to five security standards (i.e., NIST SP 800-160, NIST SP 800-30 rev.1, NIST SP 800-27 rev.A, ISO/IEC 27001 and NISTIR 8053). The contribution of this paper is a proposal of core concepts and relationships that complies with the above mentioned standards and allow to build a new security ontology.

Keywords: Security Ontology · Concepts · Relationships · Security Standards · Ontologies

1 Introduction

An ontology presents knowledge in a structured way and supports communication, organization, and knowledge reusability [1]. The main goals of an ontology are to describe reality with the concepts and relationships thereof, share vocabulary, and to provide a formal description of terms to decrease language ambiguity. Many security ontologies have been proposed over the past decade, but they only cover some aspects of the security domain. A number of questions related to security ontologies still remain:

Q1. Which core concepts and relationships can be used to adequately comprehend security issues?

Q2. Which of these core concepts and relationships should be included in a security ontology?

Q3. Which core concepts are compliant with security standards?

We conduct a systematic literature review of existing security ontologies. Since different ontologies may propose different definitions to explain concepts and relationships, systematic literature can indicate and facilitate the extraction of common core concepts and relationships that should be included in a security ontology [2].

The need for security is fundamental and includes many concepts and relationships, so engineering a security ontology is a considerable, but worthwhile challenge [3]. The concepts and relationships delineated in a security ontology should be detailed, and the concepts should be mapped to existing security standards in order to reduce ambiguities in the development thereof (e.g., differences in definitions used, incomplete ontologies).

This paper presents a systematic literature review that offers an overview of research on existing security ontologies to identify the core concepts and relationships and map them to the following five security standards: (i.e., NIST SP 800-160 [4], NIST SP 800-30 rev.1 [5], NIST SP 800-27 rev.A [6], ISO/IEC 27001 [7], and NISTIR 8053 [8]). These standards were selected because they facilitate the exchange of knowledge by ensuring a common understanding of concepts and definitions.

The aim of this paper is to review and analyze selected security ontologies and to extract the core concepts and relationships that capture security issues. The contribution of this paper is a proposal of core concepts and relationships that that complies with the above mentioned standards and can be used to develop a novel security ontology.

The remainder of this paper is structured as follows: Section 2 provides background of security ontologies. The protocol and results of the systematic literature review are detailed in Section 3. Section 4 describes studies that are related to our work. Section 5 presents conclusions and further research directions.

2 Background

This sections introduces the necessary background on existing security ontologies.

2.1 Security Ontologies

Security-related issues are critical in all contexts related to the exchange of personal data and confidential information. For a System-of-Systems (SoS), as an example, there are features of significant concern related to multiple iterations between humans, autonomous vehicles, and technology, and the heterogeneity of different autonomous vehicles that are connected with various forms of technology. In these situations, it is crucial to verify the security and privacy of services and applications to ensure that the SoS functions properly. There are potentially several and wide-ranging problems, especially when security concepts are misunderstood or misinterpreted. For this reason, an ontology can be broadly used to organize a specific area of interest.

Several ontologies have been proposed in literature to resolve security-related issues; each ontology varies according to the complexity of the specific problem, the amount of detail needed and the area that the ontology is intended to cover. For instance, one of the earliest works related to the security domain described the concepts of an information system and proposed a language, Telos, for the information system knowledge. The authors of this study emphasized that Telos can also be used for the purpose of security specification [9].

Landwehr et al. provided a taxonomy of different security flaws in computer programs [10]. A broad and abstract taxonomy describing the security concepts that includes the idea of faults, fault tolerance techniques, fault modes, and verification approaches has also been proposed [11]; this taxonomy is not exhaustive and is somewhat restricted in terms of its ability to classify actual attacks due to limited relationships among the different classes [12].

Many studies have highlighted the need for a security ontology, rather than a taxonomy of the security domain [13]. Blanco et al. listed several security ontologies in their work [14]; some of these only focused on one area of the information-security domain, while others provided an overview of information security, but nothing that is specific enough for this purpose.

Among the general ontologies that are relevant to this discussion is the proposal for the Web Ontology Language (OWL)-based ontology for information security [15], which provides an expandable ontology for the information-security domain that consists of domain-specific terminology and general concepts (e.g. top-level concepts, such as assets, threats, vulnerabilities, and countermeasures) and domain-specific technical vocabulary. Similarly, Blanco et al. suggested an ontology that models a larger portion of the information-security domain and includes non-core concepts like organizational infrastructure [14]; this ontology includes high-level concepts, such as assets, control, organization, threats, and vulnerabilities. While both of these ontologies are interesting, neither of them is exhaustive or sufficiently comprehensive; the former provides a clear and simple ontology that explains threat concepts, and the latter proposes a more complex ontology to explain asset-related concepts. This lack of specificity is covered by other security-domain-specific ontologies, e.g., [16, 17].

With this in mind, it is advisable to consider reusing existing ontologies to develop a more complete ontology that is capable of covering multiple security-related issues [18].

3 The Systematic Literature Review

In this section, the procedure for conducting the systematic literature review is explained. The systematic literature review is based on the original guidelines proposed by Kitchenham [19] and was divided into three stages:

1. Planning - questions that need to be answered by the systematic literature review were formed, and a review protocol was defined that sets out the main procedures to be followed during the review,

2. Conducting - secondary sources and studies were selected, inclusion and exclusion criteria were defined, and all the relevant papers were extracted. All duplicate search results were removed, then the results were screened through inclusion/exclusion criteria.

3. Reporting - data synthesis was performed (i.e. the studies were classified), and the questions formed in the first stage were answered.

3.1 Planning the Systematic Literature Review

Formulating the Systematic Literature Review Questions

The formulation of the questions serves to introduce the systematic literature review methodology [19]. Therefore, we formed the following three questions to identify the core security concepts and relationships that were presented in the literature:

Q1. Which core concepts and relationships can be used to adequately comprehend security issues?

Q2. Which of these core concepts and relationships should be included in a security ontology?

Q3. Which of these core concepts are compliant with security standards?

Defining the Review Protocol

According to Kitchenham [19], the review protocol should define the methods for how the following activities are to be conducted in a systematic literature review, such as the creation of a research strategy, the selection of primary studies as well as the inclusion and exclusion criteria, the quality of the assessment criteria, data extraction, and data synthesis. Toward the end of this section, we will describe how we defined and performed each activity of this protocol.

3.2 Conducting the Systematic Literature Review

The research strategy and the selection of primary studies are presented in this stage. The research strategies' goal is to find as many studies as possible that are related to the questions posed in Section 3.1. The research process includes the selection of the literature sources, the definition of the search string, the specification of inclusion and exclusion criteria, and the conduction of the research.

Selecting of Literature Sources

The search for peer reviewed literature was conducted in the three major online databases, IEEE Xplore [20], Scopus [21] (includes: IEEE, ACM and Elsevier, Wiley and Springer), and Web of Science (includes: IEEE, ACM and Elsevier) [22]. Selected databases provide access to preview and download the abstract and full text papers. The overlapping between the databases IEEE and ACM publications is covered by Scopus and Web of Science. It allows us to reduce the risk of omitting some papers of interest. Sources from the security domain were collected, and publications related to security ontologies were selected. The selection criteria for identifying security-related concepts and the relationships among them were based on the existing definitions and descriptions of these concepts and relationships.

Search String

Following [19], we derived the primary search string from the questions. Specifically, we used the "Boolean AND" to link the primary search string and the "Boolean OR" to include alternative synonyms of such search string. We used wildcard such as an asterisk(*) in the search string for multiple character searching (e.g., ontolog*, securit*, cyber*). We divided the search string into three parts (e.g., 1, 2.1, and 2.2.) in the IEEE database because the number of wildcards is limited to 7 per search. Papers published as conference articles, journal papers, or book chapters in the computer science domain between January 1990 and December 2020 were selected. Table 1 presents the search string used in the titles and abstracts that we defined in the each database and number of papers that have remained in the search.

Conducting of the Research Process

The research process was carried out in two steps. First, we used the aforementioned electronic databases and only selected papers with titles and abstracts that were deemed relevant according to the search string. In the second step, we applied the inclusion and exclusion criteria to selected papers.

Primary Selection - Inclusion and Exclusion Criteria

The research of the selected databases returned 6279 relevant papers from which we removed 1618 duplicate search results. We focused on analyzing titles and abstracts of the returned papers to discover how the concepts relate to security. Then, we applied the primary selection criteria to the remaining 4661 papers.

Inclusion criteria:

- papers are published in the English language;

- papers that present the development, creation, extension and comparison/review of ontology(ies) that cover different aspects related to security

Table 1: The search string with the results

Database	**Search String**	**Results**

IEEE	1.(("Document Title": Ontolog*) AND ("Document Title": Securit* OR "Document Title": threa* OR "Document Title": vulnerability OR "Document Title": privacy OR "Document Title": attack OR "Document Title": confidentiality OR "Document Title": integrity OR "Document Title": asset OR "Document Title": countermeasure OR "Document Title": control OR "Document Title": consequence OR "Document Title": cyber*))
	2.1. (("Abstract": Ontolog*) AND ("Abstract": Securit* OR "Abstract": threa* OR "Abstract": vulnerability OR "Abstract": privacy OR "Abstract": attack OR "Abstract": confidentiality))
	2.2.(("Abstract": Ontolog*) AND ("Abstract": integrity OR "Abstract": asset OR "Abstract": countermeasure OR "Abstract": control OR "Abstract": consequence OR "Abstract": cyber*))
		2059

Scopus	(ABS(((ontolog*) AND ((securit*) OR (threa*) OR vulnerability OR privacy OR attack OR confidentiality OR integrity OR asset OR countermeasure OR control OR consequence OR (cyber*)))) AND TITLE (((ontolog*) AND ((securit*) OR (threa*) OR vulnerability OR privacy OR attack OR confidentiality OR integirty OR asset OR countermeasure OR control OR consequence OR (cyber*))))) AND PUBYEAR > 1989 AND PUBYEAR < 2021 AND (LIMIT-TO (SUBJAREA, "COMP")) AND (LIMIT-TO (DOCTYPE, "cp") OR LIMIT-TO (DOCTYPE, "ar") OR LIMIT-TO (DOCTYPE, "ch")) AND (LIMIT-TO (LANGUAGE, "English"))	646
Web of Science	(SU=Computer Science AND (((TI=Ontolog*) AND (TI=(Securit*) OR TI=(threa*) OR TI=(vulnerability) OR TI=(privacy) OR TI=(attack) OR TI=(confidentiality) OR TI=(integrity) OR TI=(asset) OR TI=(countermeasure) OR TI=(control) OR TI=(consequence) OR TI=(cyber*))) OR ((AB=(Ontolog*)) AND (AB=(Securit*) OR AB=(threa*) OR AB=(vulnerability) OR AB=(privacy) OR AB=(attack) OR AB=(confidentiality) OR AB=(integrity) OR AB=(asset) OR AB=(countermeasure) OR AB=(control) OR AB=(consequence) OR AB=(cyber*)))))	3575
Total		**6279**

- papers are related to any of the questions from Section 3.1;
- papers are published from January 1990 to December 2020.

Exclusion criteria:

- papers that are published in languages other than English;
- papers are not available;
- papers that present an ontology or an ontology-based approach that is not related to security
- gray literature papers;
- work-in-progress papers;
- papers that are not related to any of the questions from Section 3.1;

- multiple versions or continuations of the same papers (only the complete versions were included).

Using the above-mentioned inclusion and exclusion criteria, 4505 papers were excluded, and 156 papers were analyzed.

Quality Assessment

The quality assessment criteria were applied to the 156 papers obtained from the aforementioned steps. These criteria were also applied to an additional 21 papers that were identified from obtained comparisons, reviews, and surveys. To identify the relevant papers that can be used to answer questions from Section 3.1, we formed the three following quality assessment (QA) questions:

QA1. Are the presented concepts and relationships clearly defined and described?

QA2. Do the papers present an appropriate way for the concepts and relationships to deal with security issues?

QA3. Have the concepts and relationships been justified by sufficient analysis or examples?

The quality assessment is made on the basis of full text papers. To assess the paper's completeness and relevance, each QA has only two answers, "Yes" or "No". If the answer is "No" to any one of the quality assessment questions, the paper is excluded. As a result, 169 papers were excluded, and 8 eligible papers were selected. The results of the QA of the papers are presented in Table 2.

Table 2: The results of the Quality Assessment of the papers

Author (Year)	**Title**	**Amount of core concepts**	**Amount of core relationships**
Schumacher (2003) [23]	*Towards a Security Core Ontology*	9	12
Dritsas et al.(2005) [24]	*Employing ontologies for the development of security critical applications*	7	8
Herzog et al. (2007) [15]	*An Ontology of Information Security*	6	4
Fenz and Ekelhart (2009) [25]	*Formalizing information security knowledge*	11	12
Wang and Guo (2010) [26]	*An ontological approach to computer system security*	12	10
Pereira et al. (2012) [27]	*An ontology approach in designing security information systems to support organizational security risk*	8	12
Ramanauskaite et al. (2013) [28]	*Security ontology for adaptive mapping of security standards*	5	5
Agrawal (2016) [29]	*Towards the Ontology of ISO/IEC 27005:2011 Risk Management Standard*	11	11

3.3 Reporting the Systematic Literature Review

In the final stage, the summary of the results is included, and it consists of three steps: 1) data synthesis; 2) summarizing of the results; 3) answers to the questions from Section 3.1.

Data Synthesis - Classification of Studies

The data related to QA1 was extracted directly from the list of selected papers presented in Table 2. To answer QA2, the contents of the 8 selected papers were further analyzed to identify the core concepts and relationships. The collected core concepts and relationships are presented in Table 3. In addition, we identified the core concepts and relationships that should be included in a security ontology, and described them in Section 3.3. To answer QA3, the core concepts shown in Table 4 were mapped to the definitions proposed in the security standards.

Summary of results

The results of the systematic literature review are summarized below and presented in Fig.1. The search in three databases returned total 6279 papers. From 6279 results, 1618 duplicate search results were removed. During title and abstract review of 4661 papers, 4505 articles were excluded based on inclusion/exclusion criteria. A total of 156 papers were assessed for eligibility in the systematic literature review. Twenty-one additional papers were identified from obtained reviews, comparisons, and surveys. Based on the quality assessment, 169 papers were excluded, and only 8 papers that met the criteria were included in the systematic literature review.

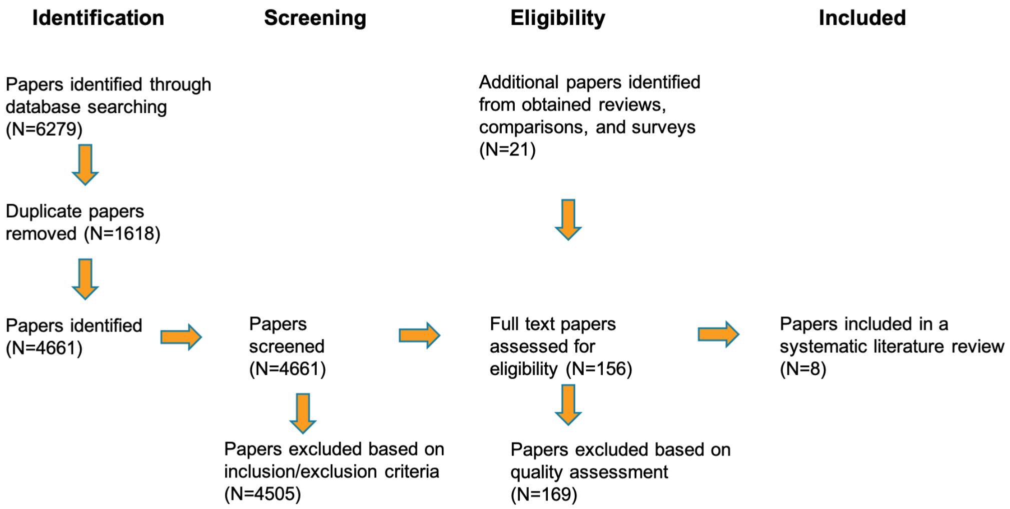
Identification
Screening
Eligibility
Included
Papers identified through database searching (N=6279)
Duplicate papers removed (N=1618)
Papers identified (N=4661)
Papers screened (N=4661)
Papers excluded based on inclusion/exclusion criteria (N=4505)
Additional papers identified from obtained reviews, comparisons, and surveys (N=21)
Full text papers assessed for eligibility (N=156)
Papers excluded based on quality assessment (N=169)
Papers included in a systematic literature review (N=8)

Fig. 1: Papers screening and selection process

Below is a short summary of the 8 papers:

Schumacher [23] proposed a security ontology with nine concepts and 12 relationships for maintaining the security pattern repositories using a general security pattern search engine.

Dritsas et al. [24] proposed a specialized security ontology with seven core concepts and eight relationships for the e-poll domain and presented how the ontology can help developers working in software projects to deal with a wide range of security issues.

Fenz and Ekelhart [25] proposed a security ontology with 11 concepts and 15 relationships that provides a unified and formal knowledge for the information security domain.

Herzog et al. [15] proposed a Web Ontology Language (OWL)-based ontology of information security overview to model security concepts, such as assets, countermeasures, threats, vulnerabilities, and their relationships. This ontology includes six core concepts and seven relationships, and can be used for reasoning about the relationships between concepts and can help determine threats that might be compromising the assets.

Wang and Guo [26] proposed the ontology for vulnerability management (OVM) with six concepts and nine relationships, which captures the core concepts of information security and focuses on software vulnerabilities.

Table 3: Security concepts and relationships used to capture security issues

Author	**Concepts**	**Relationships**
Schumacher [23]	asset, attack, attacker, countermeasure, risk, security objective, stakeholder, threat, vulnerability	*address, carry out, cause harm to, exploits, express, has, implements, increases, place value on, protect against, realizes, reduces*
Dritsas et al. [24]	asset, attacker, deliberate attack, countermeasure, objective, stakeholder, threat	*address, damages, defines, implements, protects, realizes, threatens, uses*
Herzog et al. [15]	asset, countermeasure, defense strategy, security goal, threat, vulnerability	*EnabledBy, has, protects, threatens*
Fenz and Ekelhart [25]	asset, control, control type, organization, security attribute, severity scale, standard control, threat, threat origin, threat source, vulnerability	*affects, correspondsTo, gives rise to, has, isExploitedBy, isImplementedBy, isMitigatedBy, isOwnedBy, of, on, requires, threatens*
Wang and Guo [26]	attack, attacker, consequence, countermeasure, IT_Product, vulnerability	*attack, beExploitedBy, causes, conducts, has, hasAffecteed, hasRelated, mitigates, protects*
Pereira et al. [27]	asset, attack, CIA, control, event, incident, threat, vulnerability	*areEffectedBy, detects, effects, explores, has, isMadefrom, lostOf, materialized, protects, reduces, responds, towards*
Ramanauskaite et al. [28]	asset, countermeasure, organization, threat, vulnerability	*eliminates, existsIn, exploits, has, mitigates*
Agrawal [29]	asset, CIA (confidentiality, integrity, availability), consequence, control, event, likelihood, objective, organization, risk, threat, and vulnerability	*affects, causes, contains, exploits, harms, has, isRealizedBy, leadsTo, mitigates,modifies, owns*

Pereira et al. [27] proposed a security ontology with eight concepts and 16 relationships to support organizations in dealing with the many security information issues and implementing appropriate management to facilitate their security decision-making needs. This ontology aims to unify the concepts and terminology of information security according to the ISO/IEC_JTC1 [30].

Ramanauskaite et al. [28] proposed a security ontology with five concepts and six relationships that maps various security standards (e.g., ISO 27001 [7], ISSA 5173 [31], NISTIR 7621 [32], and PCI DSS [33]). These standards are mapped to optimize the use of multiple security standards in organizations and minimize the complexity of mapping.

Agrawal [29] proposed an ontology that defines the concepts of ISO 27005 [17], including risk management standards and relationships. This ontology includes 11 concepts and 17 relationships, and enables a better understanding and identification of the core concepts of ISO 27005 [17].

Answers to the Quality Assessment Questions

This section includes the answers and the findings of this systematic literature review. First, we answered the questions in Section 3.1, and then, we presented the findings of this systematic literature review.

Q1. Which core concepts and relationships can be used to adequately comprehend security issues?

We thoroughly analyzed each of the 8 selected papers to identify any concepts and relationships that can be used to capture any security issues. The results include the concepts and relationships described in Section 3.3 that have been identified in each selected paper. As a result, 27 unique concepts and 52 relationships were identified.

Q2. Which of these core concepts and relationships should be included in a security ontology?

Among the 27 identified concepts and 52 relationships, we have selected 12 core concepts and 31 relationships that should be included in a security ontology. Each of the selected concepts and relationships was selected based on the following three criteria: 1) its relevance for capturing security issues; 2) limitation to a high-level of abstraction (e.g., system-level concepts) and 3) the frequency of its appearance in the selected papers. The following concept/relationship (frequency of appearance) were selected:

Core concepts: Asset (7), Attack (3), Attacker (3), Consequence (2), Control (3), Countermeasure (5), Event (2), Incident (1), Organization (3), Security Goal (1), Threat (7), Vulnerability (7).

Core relationships: *affects*(3), *causes*(2), *conducts*(1), *detects*(2), *eliminates*(1), *exists in*(1), *exploits*(3), *gives raise to*(1), *has*(14), *is exploited by*(2), *is implemented by*(1), *is made from*(1), *is owned by*(1), *materialized*(1), *mitigates*(4), *modifies*(2), *owns*(1), *protects*(8), *realizes*(2), *reduces*(2), *requires*(2), *threatens*(4), *towards*(1).

Q3. What are the core concepts that are compliant with security standards? We answered this question by comparing the definitions of the concepts collected from the selected papers with the definitions proposed in the security standards. As the definitions described in the standards are more detailed, a mapping of definitions from the standards to the core concepts collected from the analyzed papers is needed. The concept mapping is presented in Table 4. Only 12 core concepts could be mapped to the definitions from the security standards. The concepts of Asset, Consequence, Control, Countermeasure, Event, Incident, Organization and Vulnerability are mapped to the standards ISO/IEC 27001 [7] and NIST SP 800-160 [4]. A concept of Attack is mapped to the standards ISO/IEC 27001 [7] and NIST SP 800-30 rev.1 [5]. The concepts of Attacker and Threat are mapped to the standard NISTIR 8053 [8]. A concept of Security Goal is mapped to the standard

Table 4: Definitions of the core concepts mapped to security standards

Definitions of core concepts	**Security standard**
An asset is any resource (i.e., a tangible (furniture) or intangible (data)) that has importance and value to the owner, which may be the target of a security incident. It can exhibit some weaknesses that make assets susceptible to exploitation.	NIST SP 800-160
An attack is an unauthorized access to or use of an asset, or an attempt to expose, destroy, disable, alter, gain, or steal an asset that an attacker can take by exploiting any vulnerability and producing security events.	NIST SP 800-30 ISO/IEC 27001
An attacker is anyone or anything that attempts to expose, destroy, disable, alter, gain, or steal an asset by exploiting any vulnerability and producing some security events.	NISTIR 8053
A consequence is the possible outcome of an attack or an event (e.g., data modification, denial of services), affecting the properties (CIA) of an asset or a security incident caused by an attacker.	NIST SP 800-160 ISO/IEC 27001
A control is a mean of managing risk (e.g., policies), which can be of an administrative, technical, managerial, or legal nature. An attribute assigned to an asset reflects its relative importance or necessity in achieving or contributing to stated goals.	NIST SP 800-160 ISO/IEC 27001
A countermeasure is a prevention mechanism that detects an incident/event, reduces or avoids a threat/an incident's effects, and/or protects an asset and its properties. It can be an action/approach that mitigates or prevents the risk and impacts of an attack or a measure that modifies risk and mitigates defined vulnerabilities by implementing physical or organizational measures.	NIST SP 800-160
An event is an occurrence or change of a particular set of circumstances.	NIST SP 800-160 ISO/IEC 27001
An incident is an anomalous or unexpected event, set of events, a condition, or situation at any time during the life-cycle of a project, product, service, or system.	NIST SP 800-160 ISO/IEC 27001
An organization is a group of people and facilities with responsibilities, authorities, and relationships.	NIST SP 800-160 ISO/IEC 27001
A security goal includes confidentiality, availability, integrity, accountability, assurance, anonymity, authentication, authorization, correctness, identification, non-repudiation, policy compliance, privacy, secrecy, and trust.	NIST SP 800-27
A threat is a potential cause of an unwanted incident which can harm a system/organization/asset. It includes the types of dangers against a given set of security properties (CIA) and can be classified as passive, active, natural, accidental, and intentional.	NISTIR 8053 ISO/IEC 27001
A vulnerability is any weakness of an asset or the system that can be exploited by a threat (e.g., security flaws). It can be influenced directly (intentionally malicious) or indirectly (an unintentional mistake) by human behavior.	NIST SP 800-160 ISO/IEC 27001

NIST SP 800-27 Rev.A [6]. Based on the systematic literature review results, we identified a set of core concepts and relationships among them that were used to capture security issues and should be included in a security ontology. We mapped the collected security concepts to the definitions proposed by the security standards. The obtained 12 core concepts: **asset, attack, attacker, consequence, control, countermeasure, event, incident, organization, security goal, threat**, and **vulnerability**, and their relationships that can be used to develop a new security ontology.

4 Related Work

In this section, existing systematic literature reviews of security ontologies will be presented.

4.1 Existing systematic literature review of security ontologies

Ontologies are used in the security domain to obtain, manage, and share information and security knowledge and can be divided into two categories: general and security-specific [34,35]. The goal of security ontologies is to develop common, unambiguous semantic models of security domain concepts that reduce language ambiguity, while at the same time providing a means for easy expansion and usability of relevant knowledge in research [35,36].

Nguyen [35] presented a basic review of ontology as it relates to security information systems. The aim of this research was to investigate the literature and identify areas of interest for further research. The author concluded that at that time, there were no ontologies for use in the modeling and security of computer networks.

Souag et al. [34] conducted a systematic literature review to identify existing research on ontologies and the requirements and security issues thereof. They proposed eight categories according to which security ontologies could be classified: theoretical basis, security taxonomies, general, specific, risk-based, web-oriented, requirements-related, and modeling. The authors only found a few studies related to security ontologies that offered different methods to cover security issues; each ontology was analyzed for the manner in which it covered a specific issue and to determine whether it could be used to define security requirements. This analysis revealed a gap between ontology and security-engineering domains.

Blanco et al. [14] performed a systematic literature review to identify, analyze, and extract the main security ontologies related to the information security domain. They only considered titles, keywords, and abstracts when analyzing these papers, and they concluded that the literature could be classified into three groups: seventeen were general and specific security ontologies, nine were semantic web-oriented ontologies, and four were theoretical papers. The authors discovered that existing security ontologies do not exhaustively define concepts, do not use appropriate descriptive language for descriptions and cannot be extended or reused.

Three years after publishing this review, Blanco et al. [37], conducted an extended systematic literature review that included their earlier analysis and a comparison of the security ontologies detailed therein. The aim of this research was to identify and classify the purpose of each study; titles, keywords, and abstracts were analyzed and delineate relationships between ontological concepts used in security domains, but security standards were not considered in this analysis. The investigation resulted in eight general and 20 security-specific ontologies, and three theoretical papers. The authors concluded that these ontologies contributed to the security domain, but only provided a partial solution, rather than an integrated security ontology. They also determined that successfully implementing an integrated ontology was a complex task that required more in-depth study.

While these studies classified, analyzed, and reviewed several existing security ontologies, they did not cover the entire spectrum of security knowledge; we will therefore include as many security-knowledge resources as we can in this study in order to identify the core concepts and relationships thereof. Moreover, because these studies focused on information system security, rather than general security, our goal is not to compare different security ontologies, but rather to integrate existing ontologies to create an appropriate new security ontology.

The aforementioned reviews were related to the security aspects of application-specific domains, and they did not include the security standards we use for ontology creation; in contrast, our approach, considers various security ontologies and is therefore general enough to be applicable to any IT system. Even though the cited research did not examine any ontological concepts mapped to security standards, we were able to use these studies to identify the core concepts and relationships for various security issues. We then mapped these concepts to the appropriate security standards, which is presented in Section 3.3.

The contributions of this study differs from previous efforts:

- Core concepts and relationships that capture security issues were identified,
- Already-developed security ontologies were reused without being redefined,
- Core concepts were mapped to existing security standards,
- Security knowledge was considered in order to reuse and expand previously collected knowledge.

5 Conclusions and future work

We conducted a systematic literature review of the existing security literature to identify the core concepts for capturing security issues and the relationships thereof. Overall, we included 156 papers in this review, and we examined all of these with three quality assessment criteria questions in mind. As a result, 8 eligible papers were selected and used for further analysis, and we presented the selected data. Effective presentation of the set of selected data was made using tables.

We concluded that the existing ontologies are not appropriate, lack the core concepts, and do not fully comply with existing security standards. We then identified a set of core concepts and relationships that capture security issues. The definitions of these 12 core concepts were mapped to security standards. The aim of this paper was to review and analyze selected security ontologies and to extract core concepts and relationships that capture security issues. The contribution of this paper proposes the core concepts and relationships that comply with the above mentioned standards and allow to develop a new security ontology that can be evaluated and compared to other ontologies. We will therefore develop a security ontology that is based on a foundational ontology and integrates several general and security-specific ontologies, and is able to cover multiple aspects related to security, including the security of autonomous vehicles in an System-of-Systems (SoS).

6 Acknowledgment

This work is supported by the Serendipity project funded by the Swedish Foundation for Strategic Research (SSF) and also by the DPAC project funded by the Knowledge foundation (KK-Stiftelsen).

References

1. Gruber, T.R.: Toward principles for the design of ontologies used for knowledge sharing? International journal of human-computer studies, **43**(4-5) 907–928 (1995)
2. Kang, W., Liang, Y.: A security ontology with MDA for software development. In: International Conference on Cyber-Enabled Distribitued Computing and Knowledge Discovery (CyberC), pp. 67–74, IEEE, Beijing (2013)
3. Tsoumas, B., Gritzalis, D.: Towards an ontology-based security management. In: 20th International Conference on Advanced Information Networking and Applications (AINA), pp. 985–992. IEEE, Vienna (2006)
4. Ross, R.S., McEvilley, M., Oren, J.C.: Systems security engineering: Considerations for a multidisciplinary approach in the engineering of trustworthy secure systems. Special Publication (NIST SP)-800-160, (2016)
5. National Institute of Standards and Technology NIST SP 800-30 Revision 1: Guide for Conducting Risk Assessments, 1 (2), pp. 1–95 (2012)
6. Stoneburner, G., Hayden, C., Feringa, A.: SP 800-27 Rev. A. Engineering Principles for Information Technology Security (A Baseline for Achieving Security), (2017)
7. ISO/IEC 27001:2013 - Information security management system - requirements
8. Garfinkel, S.L.: De-Identification of Personal Information. NIST Interagency/Internal Report (NISTIR). 8053, (2015)
9. Mylopoulos, J., Borgida, A., Jarke, M., Koubarakis, M.: Telos: Representing Knowledge About Information Systems. ACM Trans. Inf. Syst., **8**(4), 325–362 (1990)
10. Landwehr, C.,E., Bull, A.,R., McDermott, J.,P., Choi, W.,S.: A taxonomy of computer progrxam security flaws. ACM Comput. Surv., **26**(3), 211–254 (1994)
11. Avizienis, A., Laprie, J.C., Randell, B., Landwehr, C.: Basic concepts and taxonomy of dependable and secure computing. IEEE Transactions on Dependable and Secure Computing, **1**(1), 11–33 (2004)
12. Howard, J.,D., Longstaff, T.: A common language for computer security incidents, Sandia National Laboratories, 1–25 (1998)
13. Donner, M.: Toward a Security Ontology. IEEE Security and Privacy, **1**(3), 6–7 (2003)
14. Blanco, C., Lasheras, J., Valencia-Garcia, R., Fernandez-Medina, E., Toval, A., Piattini, M.: A Systematic Review and Comparison of Security Ontologies, In: 3rd International Conference on Availability, Reliability and Security (ARES), pp. 813–820. IEEE, Barcelona (2008)
15. Herzog, A., Shahmehri, N. Duma, C.: An Ontology of Information Security. Int. J. Inf. Secur. Priv., **1**(4), 1–23 (2007)
16. Geneiatakis, D., Lambrinoudakis, C.: An ontology description for SIP security flaws. Computer Communications, **30**(6), 1367–1374 (2007)
17. Undercoffer, J., Joshi, A., Pinkston, A.: Modeling Computer Attacks: An Ontology for Intrusion Detection. In: Vigna, G., Kruegel, C., Jonsson, E. (eds.) Recent Advances in Intrusion Detection. RAID 2003. LNCS, vol. 2820, pp. 113-135, Springer, Heidelberg. (2003). https://doi.org/10.1145/1533057.1533084
18. Noy, F., N., McGuinness D., L.: Ontology development 101: A guide to creating your first ontology, pp. 1–25, (2001)
19. Kitchenham, B.: Procedures for performing systematic reviews. Keele, UK, Keele University, **33**(2004), 1–26 (2004)
20. IEEE Xplore, `https://ieeexplore.ieee.org/Xplore/home.jsp.`. Last accessed 20 Feb 2021
21. Scopus, `https://www.scopus.com/search/form.uri?display=basic`. Last accessed 20 Feb 2021
22. Web of Science, `https://apps-webofknowledge-com.ep.bib.mdh.se/WOS_GeneralSearch_input.do?product=WOS&SID=F5zJQFlTESs3EdPTTZH&search_mode=GeneralSearch`. Last accessed 20 Feb 2021
23. Schumacher, M.: 8. A Theoretical Model for Security Patterns. In: Security Engineering with Patterns. LNCS, vol. 2754. pp. 121–140, Springer, Heidelberg (2003). https://doi.org/10.1007/978-3-540-45180-8_8

24. Dritsas, S., Gymnopoulos, L., Karyda, M., Balopoulos, T., Kokolakis, S., Lambrinoudakis, C., Gritzalis, S.: Employing Ontologies for the Development of Security Critical Applications: The Secure e-Poll Paradigm. IFIP Advances in Information and Communication Technology. Vol. 189, pp. 187–201, Springer, Boston, MA. (2005) https://doi.org/10.1007/0-387-29773-1_13
25. Fenz, S., Ekelhart, A.: Formalizing information security knowledge. In: 4th International Symposium on Information, Computer, and Communications Security (ASIACCS), pp. 183–194. ACM, New York (2009)
26. Wang, J.,A., Guo, M.: OVM: an ontology for vulnerability management. In: 5th Annual Workshop on Cyber Security and Information Intelligence Research: Cyber Security and Information Intelligence Challenges and Strategies (CSIIRW), pp.34:1-34:4. ACM, New York (2009)
27. Pereira, T., Santos, H.: An Ontology Approach in Designing Security Information Systems to Support Organizational Security Risk Knowledge. In: Proceedings of the International Conference on Knowledge Engineering and Ontology Development (KEOD), Vol. 1, SSEO, pp. 461–466, ScitePress, Barcelona, Spain (2012)
28. Ramanauskaite, S., Olifer, D., Goranin, N., Cenys, A.: Security ontology for adaptive mapping of security standards. Int. J. Comput. Commun. (IJCCC), **8**(6), 813–825 (2013)
29. Agrawal, V.: Towards the Ontology of ISO/IEC 27005: 2011 Risk Management Standard. HAISA, 101–111 (2016)
30. ISO/IEC_JTC1, 2008. ISO/IEC FDIS 27001:2005 Information Technology - Security Techniques - Information Security management Systems - Requirements, Geneva, Switzerland.
31. ISSA. 5173 Security Standard for SMEs. `http://www.wlan-defence.com/wp/ISSA-UK.pdf`
32. Paulsen, C., Toth, P.: Small Business Information Security: The Fundamentals, NIST Interagency Report 7621, Revision 1, Gaithersburg, Md. (2016)
33. PCI DSS. Requirements and Security Assessment Procedures, PCI Security Standards Council. Wakefield, MA. USA. 2008
34. Souag, A., Salinesi, C., Comyn-Wattiau, I.: Ontologies for security requirements: a literature survey and classification. In: Bajec, M., Eder, J. (eds.) CAiSE Workshop 2012. LNBIP, vol. 112, pp. 61–69, Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-31069-0
35. Nguyen, V.: Ontologies and Information Systems: A Literature Survey, DSTO-TN-1002, Defence Science and Technology Organisation, pp. 66–92, Edingubrgh, SA (2011)
36. Boinski, T., Orlowski, P., Szymanski, J., Krawczyk, H.: Security Ontology Construction and Integration. In: Filipe, J., Dietz, J.L.G. (eds.) International Conference on Knowledge Engineering and Ontology Development (KEOD), pp. 369–374. INSTICC, Paris (2011)
37. Blanco, C., Lasheras, J., Fernandez.Medina, E., Valencia-Garcia, R., Toval, A.: Basis for an integrated security ontology according to a systematic review of existing proposals. Comput. Stand. Inter. **33**, 372–388 (2011)