


# Security Ontologies: A Systematic Literature Review

Malina Adach <sup>[0000-0002-7986-2214]</sup>, Kaj Hänninen<sup>[0000-0003-0757-822X]</sup>, and  
Kristina Lundqvist<sup>[0000-0003-0904-3712]</sup>

School of Innovation, Design and Engineering, Mälardalen University, Västerås,  
Sweden

{malina.adach, kaj.hanninen, kristina.lundqvist}@mdh.se

**Abstract.** Security ontologies have been developed to facilitate the organization and management of security knowledge. A comparison and evaluation of how these ontologies relate to one another is challenging due to their structure, size, complexity, and level of expressiveness. Differences between ontologies can be found on both the ontological and linguistic levels, resulting in errors and inconsistencies (i.e., different concept hierarchies, types of concepts, definitions) when comparing and aligning them. Moreover, many concepts related to security ontologies have not been thoroughly explored and do not fully meet security standards. By using standards, we can ensure that concepts and definitions are unified and coherent. In this study, we address these deficiencies by reviewing existing security ontologies to identify core concepts and relationships. The primary objective of the systematic literature review is to identify core concepts and relationships that are used to describe security issues. We further analyse and map these core concepts and relationships 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). As a contribution, this paper provides a set of core concepts and relationships that comply with the standards mentioned above and allow for a new security ontology to be developed.

**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 avoid language ambiguity. Many security ontologies have been proposed over the past decade, but they only cover some aspects of the security domain. Several questions related to security ontologies still remain, for example:

*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?*

In this study, we conduct a systematic literature review of existing security ontologies. Since different ontologies may propose different definitions to explain concepts and relationships, a systematic literature review 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 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: 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.

Developing a System-of-System with compliance standards improves security, and this was the reason for mapping identified concepts to common security standards. The mapping of security standards can help ontologies to be optimized by identifying concepts compatible with security standards and removing redundant security measures to meet those standards. Existing security ontologies can be used to simplify the mapping of more than two security standards. Since security ontologies cover a wide range of areas, they play a significant role in mapping. Consequently, their concepts must be detailed and described to comply with security standards. The contribution of this study differs from previous efforts in the following ways:

- 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 to reuse and expand previously collected knowledge

The reason we studied these ontologies to find common themes is that we need to identify security concepts and relationships that can be mapped to security standards. The main contribution of this paper is a proposal of core concepts and relationships 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 describes background on security ontologies and studies that are related to our work. The process of the systematic literature review and analysis of the results are detailed in Section 3. Section 4 presents conclusions and further research directions.

## 2 Background and related work

This section 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 [9]. 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 relate to 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 function properly. There are potentially several and wide-ranging problems, especially when security concepts are misunderstood or misinterpreted [10]. 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 [11]. Landwehr et al. provided a taxonomy of different security flaws in computer programs [12]. 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 [13]; 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 [14]. Many studies have highlighted the need for a security ontology, rather than a taxonomy of the security domain [15]. Blanco et al. listed several security ontologies in their work [16]; 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 based ontology for information security [17], 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 [16]; this ontology includes high-level concepts, such as assets, control, organization, threats, and vulnerabilities. While both 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., [18,19].

It is advisable to consider reusing existing ontologies to develop a more complete ontology that is capable of covering multiple security-related issues [20].

## 2.2 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 [21]. 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 [22].

Souag et al. [21] 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 way 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. Nguyen [23] 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. Blanco et al. [16] 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. [24], 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 and map them to five security standards.

### 3 The Systematic Literature Review

In this section, the procedure for conducting the systematic literature review is explained. The systematic literature review was based on the original guidelines proposed by Kitchenham [25] 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.

The scope of this review has been limited to identifying the core concepts and relationships that:

- (i) can be utilized to adequately comprehend security issues,
- (ii) should be included in a security ontology, and
- (iii) are compliant with security standards.

This study focuses on identifying and gathering concepts and relationships that can be used to develop a novel security ontology.

#### 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 [25]. 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 [25], 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. In section 3.2, 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 at this stage. The research strategy's 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 conducting of the research.

#### **Selection of Literature Sources**

The search for peer reviewed literature was conducted in the three major online databases, IEEE Xplore [26], Scopus [27] (includes: IEEE, ACM, and Elsevier, Wiley, and Springer), and Web of Science (includes: IEEE, ACM, and Elsevier) [28]. Selected databases provide access to preview and download the abstract and full text papers. The overlapping between the IEEE databases and ACM publications is covered by Scopus and Web of Science. This 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 [25], we derived the primary search string from the questions. Specifically, we used "Boolean AND" to link the primary search string and "Boolean OR" to include alternative synonyms of such a search string. We used a wildcard via an asterisk (\*) in the search string for multiple character searching (e.g., *ontolog\**, *securit\**, *cyber\**). We searched for ontologies developed both for security and cybersecurity. We divided the search string into two parts (1 and 2, differences are highlighted in bold text) in the IEEE database because the number of wildcards is limited to 7 per search. Papers published as conference

articles, journal papers, early access or book chapters in the computer science domain between January 1988 and April 2022 were selected. We used the following search strings to define the titles and abstracts in each database, and the number of papers found in the search.

**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\*)) OR ("Abstract": Ontolog\*) AND ("Abstract": **Securit\* OR "Abstract": threa\* OR "Abstract": vulnerability OR "Abstract": privacy OR "Abstract": attack OR "Abstract": confidentiality**)) - returned **1127** results.

**IEEE 2:** (("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\*)) OR ("Abstract": Ontolog\*) AND ("Abstract": **integrity OR "Abstract": asset OR "Abstract": countermeasure OR "Abstract": control OR "Abstract": consequence OR "Abstract": cyber\***)) returned **1809** results.

**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 integrity OR asset OR countermeasure OR control OR consequence OR (cyber\*)))) AND PUBYEAR > 1988 AND PUBYEAR < 2022 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"))) returned **698** results.

**Web of Science:** (SU=Computer Science AND (((TI=Ontolog\*) AND (TI=(Securit\*) OR TI=(asset) OR TI=(threa\*) OR TI=(privacy) OR TI=(attack) OR TI=(confidentiality) OR TI=(control) OR TI=(integrity) OR TI=(countermeasure) OR TI=(vulnerability) OR TI=(cyber\*) OR TI=(consequence) )) OR ((AB=(Ontolog\*)) AND (AB=(Securit\*) OR AB=(threa\*) OR AB=(vulnerability) OR AB=(privacy) OR AB=(attack) OR AB=(asset) OR AB=(integrity) OR AB=(confidentiality) OR AB=(countermeasure) OR AB=(control) OR AB=(consequence) OR AB=(cyber\*)))))) returned **3921** results.

## 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. Our review was conducted manually, and each author participated in the entire screening process. There are many security ontologies and ontological approaches represented by UML (Unified Modelling Language) class models or OWL (The Web Ontology Language), which can only be manually interpreted. Our preliminary search resulted in a total of **7,555** papers, and selection criteria were applied to these papers to obtain the final group of relevant papers. The results of searches are shown in [29]. Based on our review, we have not identified any paper strengths or weaknesses, merely focusing on our inclusion and exclusion criteria.

### Primary Selection – Inclusion and Exclusion Criteria

The research with the selected databases returned 7,555 relevant papers from which we removed **2,442** 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 (shown in Table 1) to the remaining **5,113** papers.

Table 1: Inclusion and exclusion criteria

Inclusion criteria	Exclusion criteria
Papers are published in the English language	Papers are published in languages other than English
Papers present the development or extension of ontology/(ies) or an ontology- based approach related to security and has already been used at least once	Papers present an ontology or an ontology-based approach that is not related to security
Papers present comparison/reviews/surveys of ontology/(ies) related to security	Gray literature papers, short papers or posters
Papers are published from January 1988 to April 2022	Work-in-progress papers
Papers are published and available in scientific databases or printed versions	Papers are not available
Papers are related to any of the questions from Section 3.1	Papers are not related to any of the questions from Section 3.1
Complete versions of papers	Multiple versions of the same papers
Papers have already approval by the scientific community	Papers shorter than 3 pages



This process has been performed manually with the possibility to evaluate each paper with one of three options:

1. The paper is accepted because it presents the development, extension, or comparison/ reviews/ surveys of ontology/ies or ontology-based approaches that cover different aspects related to security.

2. The paper presents an ontology or an ontology-based approach that is not related to security.

3. The paper is rejected because it does not meet criterion in 1 or 2.

After manually applying the above-mentioned three options and the inclusion and exclusion criteria presented in Table 1 to the paper's titles and abstracts, **4,914** irrelevant papers were excluded, and **199** relevant papers were analyzed in the next step.

### Quality Assessment

The quality assessment criteria were applied to the **199** papers obtained from the aforementioned steps. Furthermore, these criteria were applied to **22** additional papers that were identified through the snowballing step. To identify the relevant papers that could 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 above quality assessment criteria were applied to the full texts of **221** papers. To assess the paper's completeness and relevance, each QA had only two possible answers, "Yes" or "No." If the answer is "No" to any one of the quality assessments questions, the paper is excluded.

### 3.3 Reporting the Systematic Literature Review

In the final stage, the summary of the results is included. This consists of three steps:

1. Data synthesis
2. Results and analysis
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 Section 3.2. 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.

## Results and Analysis

The results of the systematic literature review are summarized below and presented in fig.1. The search in three databases returned total of **7,555** papers from which **2,442** duplicate search results were removed. For the review process, we have developed inclusion and exclusion criteria that we can refer to when either including or excluding a paper. The inclusion and exclusion criteria were designed to select papers that address our main research questions. Therefore, these criteria determine the scope of our review.

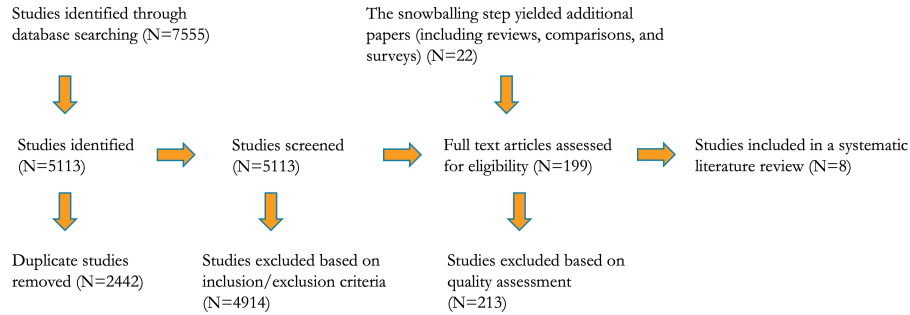


Fig. 1: Paper screening process

During title and abstract review of **5,113** papers, **4,914** articles were excluded based on inclusion/exclusion criteria. A total of **199** papers were assessed for eligibility in the systematic literature review. After applying the inclusion and exclusion criteria, the final papers were selected for quality assessment. The snowballing step yielded **twenty-two** additional papers (including reviews, comparisons, and surveys). This approach provided us with **221** papers, which were included in the quality assessment step. Based on the quality assessment from Section 3.2, **213** papers were excluded, and only **8** papers that met the criteria were included in the systematic literature review.

As a result, **8** eligible papers were selected as relevant for addressing our question from Section 3.1. The results of the QA of the papers are presented in Table 2. Below is a short summary of the 8 papers identified as relevant:

**1.Schumacher** [30] proposed a security ontology with nine concepts and 12 relationships for maintaining the security pattern repositories using a theoretical search engine to locate security patterns. Consequently, the author has focused on identifying a small number of core security concepts and limited the scope to first level of abstraction.

**2.Dritsas et al.** [31] proposed a specialized security ontology with seven core concepts and nine relationships for the e-poll domain and presented how

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

Author (Year)	Title	Number of concepts	Number of relationships
Schumacher (2003) [30]	<i>Towards a security core ontology</i>	9	12
Dritsas et al. (2005) [31]	<i>Employing ontologies for the development of security critical applications</i>	7	9
Herzog et al. (2007) [17]	<i>An ontology of information security</i>	6	7
Fenz and Ekelhart (2009) [32]	<i>Formalizing information security knowledge</i>	11	15
Wang and Guo (2010) [33]	<i>OVM: an ontology for vulnerability management</i>	6	10
Pereira et al. (2012) [34]	<i>An ontology approach in designing security information systems to support organizational security risk</i>	8	16
Ramanauskaite et al. (2013) [36]	<i>Security ontology for adaptive mapping of security standards</i>	5	7
Agrawal (2016) [37]	<i>Towards the ontology of ISO/IEC 27005:2011 risk management standard</i>	11	16

the ontology can help developers working in software projects to deal with a wide range of security issues.

**3.Fenz and Ekelhart** [32] proposed a security ontology with 11 concepts and 15 relationships that provides a unified and formal knowledge for the information security domain. Their ontology was integrated with ISO/IEC 27001 [7] standard ontology and applied to quantitative risk assessment.

**4.Herzog et al.** [17] proposed a Web Ontology Language 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.

**5.Wang and Guo** [33] proposed the ontology for vulnerability management (OVM) with six concepts and ten relationships, which captures the core concepts of information security and focuses on software vulnerabilities. The authors uti-

lized the NVD (National Vulnerability Database) to populate their ontology with descriptions of some common vulnerabilities.

**6. Pereira et al.** [34] 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 [35].

**7. Ramanauskaite et al.** [36] proposed a security ontology with five concepts and seven relationships that maps various security standards (e.g., ISO 27001 [7], ISSA 5173 [38], NISTIR 7621 [39], and PCI DSS [40]). These standards are mapped to optimize the use of multiple security standards in organizations and minimize the complexity of mapping.

**8. Agrawal** [37] proposed an ontology that defines the concepts of ISO 27005 [41], including risk management standards and relationships. This ontology includes 11 concepts and 16 relationships, and enables a better understanding and identification of the core concepts of ISO 27005 [41].

Table 3 presents core concepts and relationships that have been gathered from the eight above mentioned papers. The above 8 papers were identified as relevant in answering questions from Section 3.3. Answers were presented in the next step.

### Answers to the Review Questions

This section includes the answers and the findings of this systematic literature review. First, we answered the questions in Section 3.1. 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 could 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, a total of **63** concepts and **92** relationships were identified, among which **27** unique concepts and **51** relationships were distinguished.

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

Among the 27 identified concepts and 51 relationships, we have selected **12** core concepts and **35** relationships that should be included in a security ontology. Each of the selected concepts and relationships was selected based on the following three criteria:

- its relevance for capturing security issues;
- limitation to a high-level of abstraction (e.g., system-level concepts), and
- the frequency of its appearance in the selected papers.

The following **concepts and relationships** (frequency of appearance) were selected:

Table 3: Security concepts and relationships used to capture security issues in the identified papers

Author	Concepts	Relationships
Schumacher [30]	asset, attack, attacker, countermeasure, risk, security objective, stakeholder, threat, vulnerability	<i>address, carry out, cause harm to, exploits, express, has, implements, increases, place value on, protect against, realizes, reduces</i>
Dritsas et al. [31]	asset, attacker, deliberate attack, countermeasure, objective, stakeholder, threat	<i>address, damages, defines, implements, protects, protects, realizes, threatens, uses</i>
Herzog et al. [17]	asset, countermeasure, defense strategy, security goal, threat, vulnerability	<i>EnabledBy, has, protects, protects, protects, threatens, threatens</i>
Fenz and Ekelhart [32]	asset, control, control type, organization, security attribute, severity scale, standard control, threat, threat origin, threat source, vulnerability	<i>affects, correspondsTo, gives rise to, has, has, has, isExploitedBy, isImplementedBy, isMitigatedBy, isOwnedBy, of, on, requires, requires, threatens</i>
Wang and Guo [33]	attack, attacker, consequence, countermeasure, IT_Product, vulnerability	<i>attack, attackConsequence, isExploitedBy, causes, conducts, has, has, hasRelated, mitigates, protects</i>
Pereira et al. [34]	asset, attack, CIA, control, event, incident, threat, vulnerability	<i>areEffectedBy, detects, detects, effects, explores, has, has, isMadeFrom, lostOf, materialized, protects, protects, protects, reduces, responds, towards</i>
Ramanauskaite et al. [36]	asset, countermeasure, organization, threat, vulnerability	<i>eliminates, existsIn, existsIn, exploits, has, has, mitigates</i>
Agrawal [37]	asset, CIA, consequence, control, event, likelihood, objective, organization, risk, threat, and vulnerability	<i>affects, affects, causes, contains, exploits, harms, has, has, has, has, isRealizedBy, leadsTo, mitigates, modifies, modifies, owns</i>

**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), attackConsequence(1), causes(2), conducts(1), detects(2), eliminates(1), exists in(2), exploits(3), gives raise to(1), has(16), is exploited by(2), is implemented by(1), is made from(1), isMitigatedBy, is*

*owned by(1), materialized(1), mitigates(4), modifies(2), owns(1), protects(8), realizes(2), reduces(2), requires(2), responds(1), 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. In this step, from the 8 relevant papers core concepts were extracted and duplicates were removed. Only **12** core concepts extracted could be mapped to the definitions described 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 was needed. The concept mapping with security standards is presented in Table 4.

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]. The 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 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 can be used to develop a new security ontology.

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

Definitions of core concepts	Security standard
<b>An asset</b> 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
<b>An attack</b> 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
<b>An attacker</b> 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
<b>A consequence</b> 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
<b>A control</b> 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
<b>A countermeasure</b> 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
<b>An event</b> is an occurrence or change of a particular set of circumstances.	NIST SP 800-160 ISO/IEC 27001
<b>An incident</b> 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
<b>An organization</b> is a group of people and facilities with responsibilities, authorities, and relationships.	NIST SP 800-160 ISO/IEC 27001
<b>A security goal</b> includes confidentiality, availability, integrity, accountability, assurance, anonymity, authentication, authorization, correctness, identification, non-repudiation, policy compliance, privacy, secrecy, and trust.	NIST SP 800-27
<b>A threat</b> 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
<b>A vulnerability</b> 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

## 4 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 **221** papers in this review, and we examined all of these with three quality assessment criteria questions in mind. The selection process has been based on titles, abstracts, and full-text reading. As a result, **8** eligible papers were selected as relevant to the questions from Section 3.1 and used for further analysis, and we presented the selected data. Effective presentation of the set of selected data from the relevant papers was made using tables. Based on the results of our review, we conclude that the existing ontologies are not complete or consistent, 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 reason we studied these ontologies to find a common theme was that we needed to identify security concepts and relationships that could be mapped to security standards and compared with safety concepts and relationships. To the best of our knowledge this is the first study that maps the core concepts and relationships with common security standards. The main contribution of this paper proposes the core concepts and relationships that comply with the above-mentioned standards and allow the development of a new security ontology that can be evaluated and compared to other ontologies.

## 5 Acknowledgment

This work is supported by the projects: Serendipity - Secure and dependable platforms for autonomy, grant nr: RIT17-0009, funded by the Swedish Foundation for Strategic Research (SSF) and by the DPAC - Dependable Platform for Autonomous Systems and Control, grant nr: 20150022, funded by the Knowledge foundation (KKS).

## References

1. Gruber, T.R.: Toward principles for the design of ontologies used for knowledge sharing?. *Int. J. of hum.-comp. stud.*, **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 Distributed 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.: NIST SP 800-160, systems security engineering considerations for a multidisciplinary approach in the engineering of trustworthy secure systems, "NIST, US Department of Commerce, Gaithersburg, MD, USA, Tech. Rep. NIST SP, (2016)



5. Ross, R.S., NIST SP 800-30 REV. 1: guide for conducting risk assessments,” NIST, 2012. <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf> (accessed 14 June, 2022).
6. Stoneburner, G., Hayden, C., Feringa, A.: NIST SP 800-27 Rev. A. Engineering principles for information technology security (a baseline for achieving security), NIST, (2017)
7. ISO/IEC 27001:2013 - Information security management system - requirements, ISO, Tech. Rep., (2013)
8. Garfinkel, S.L.: NISTIR 8053: de-identification of personal information, NIST, (2015)
9. Maxwell, T.A.: Information Policy, Data Mining, and National Security: False Positives and Unidentified Negatives. In: 38th Annual Hawaii International Conference on System Sciences, pp. 134c-134c, (2005), <https://doi.org/10.1109/HICSS.2005.317>
10. Jurisica, I., Mylopoulos, J., Yu, E. Ontologies for Knowledge Management: An Information Systems Perspective. *Know. Inf. Sys.* 6, 380–401 (2004),
11. Mylopoulos, J., Borgida, A., Jarke, M., Koubarakis, M.: Telos: representing knowledge about information systems. *ACM Trans. Inf. Syst.*, **8**(4), 325–362 (1990)
12. Landwehr, C.,E., Bull, A.,R., McDermott, J.,P., Choi, W.,S.: A taxonomy of computer program security flaws. *ACM Comput. Surv.*, **26**(3), 211–254 (1994)
13. 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)
14. Howard, J.,D., Longstaff, T.: A common language for computer security incidents, Sandia National Laboratories, 1–25 (1998)
15. Donner, M.: Toward a security ontology. *IEEE Security and Privacy*, **1**(3), 6–7 (2003)
16. Blanco, C., Lasheras, J., Valencia-Garcia, R., Fernández-Medina, E., Alvarez, J., 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)
17. Herzog, A., Shahmehri, N., Duma, C.: An ontology of information security. *Int. J. Inf. Secur. Priv.*, **1**(4), 1–23 (2007)
18. 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>
19. Geneiatakis, D., Lambrinouidakis, C.: An ontology description for SIP security flaws. *Computer Communications*, **30**(6), 1367–1374 (2007)
20. Noy, F., N., McGuinness D., L.: Ontology development 101: A guide to creating your first ontology, pp. 1–25, (2001)
21. 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>
22. 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)
23. Nguyen, V.: Ontologies and information systems: A literature survey, DSTO-TN-1002, Defence Science and Technology Organisation, pp. 66–92, Edingubrgh, SA (2011)

24. Blanco, C., Lasheras, J., Fernández-Medina, E., Valencia-García, R., Toval, A.: Basis for an integrated security ontology according to a systematic review of existing proposals. *Comput. Stand. Int.* **33**, 372–388 (2011)
25. Kitchenham, B.: Procedures for performing systematic reviews. Keele, UK, Keele University, **33**(2004), 1–26 (2004)
26. IEEE Xplore, <https://ieeexplore.ieee.org/Xplore/home.jsp>. Accessed 14 June 2022
27. Scopus, <https://www.scopus.com/search/form.uri?display=basic>. Accessed 14 June 2022
28. Web of Science, [https://apps- webofknowledge-com.ep.bib.mdh.se/WOS\\_GeneralSearch\\_input.do?product=WOS&SID=F5zJQf1TESs3EdPTTZH&search\\_mode=GeneralSearch](https://apps- webofknowledge-com.ep.bib.mdh.se/WOS_GeneralSearch_input.do?product=WOS&SID=F5zJQf1TESs3EdPTTZH&search_mode=GeneralSearch). Accessed 14 June 2022
29. Adach, M., Hänninen, K., Lundqvist, K.: Search results of security ontologies 1988–2022, Tech. Rep., MDU, Västerås, [http://www.es.mdh.se/pdf\\_publications/6424.pdf](http://www.es.mdh.se/pdf_publications/6424.pdf) (accessed 14 June, 2022).
30. Schumacher, M.: 6. Towards a Security Core Ontology. 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](https://doi.org/10.1007/978-3-540-45180-8_8)
31. Dritsas, S., Gymnopoulos, L., Karyda, M., Balopoulos, T., Kokolakis, S., Lambri-noudakis, C., Gritzalis, S.: Employing ontologies for the development of security critical applications. In: *Challenges of Expanding Internet: E-Commerce, E-Business, and E-Government*, LNCS, vol. 189, pp. 187–201, Springer, Boston, MA. (2005) [https://doi.org/10.1007/0-387-29773-1\\_13](https://doi.org/10.1007/0-387-29773-1_13)
32. 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)
33. 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. Oak Ridge Tennessee, USA (2009)
34. Pereira, T., Santos, H.: An ontology approach in designing security information systems to support organizational security risk knowledge. In: *International Conference on Knowledge Engineering and Ontology Development (KEOD)*, Vol. 1, SSEO, pp. 461–466, ScitePress, Barcelona, Spain (2012)
35. ISO/IEC\_JTC1 27005:2008: information technology - security techniques - information security risk management, ISO, Tech. Rep. (2008)
36. Ramanauskaite, S., Olifer, D., Goranin, N., Cenys, A.: Security ontology for adaptive mapping of security standards. *Int. J. Comput. Commun.*, **8**(6), 813–825 (2013)
37. Agrawal, V.: Towards the ontology of ISO/IEC 27005: 2011 risk management standard. HAISA, 101–111, Frankfurt, Germany (2016)
38. ISSA-UK. Information security for small and medium-sized enterprises, Information System Security Association, Tech. Rep., (2011)
39. Paulsen, C., Toth, P.: NISTIR 7621 small business information security: The fundamentals, NIST, US Department of Commerce. (2016)
40. Payment Card and Industry. Payment card industry data security standard (PCIDSS), PCI-Security Standard Council, Tech. Rep., 2006. [https://www.commerce.uwo.ca/pdf/PCI\\_DSS\\_v3-2-1.pdf](https://www.commerce.uwo.ca/pdf/PCI_DSS_v3-2-1.pdf). Accessed 14 June 2022
41. ISO/IEC 27005:2011 - information technology — security techniques — information security risk management, ISO, Tech. Rep., (2011)