How FAIR are Security Core Ontologies?
A Systematic Mapping Study

Ítalo Oliveira, Mattia Fumagalli, Tiago Prince Sales, and Giancarlo Guizzardi

Conceptual and Cognitive Modeling Research Group (CORE)
Free University of Bozen-Bolzano, Bolzano, Italy
{idasilvaoliveira, mattia.fumagalli, tiago.princesales,
giancarlo.guizzardi}@unibz.it

Abstract. Recently, ontology-based approaches to security, in particular to information security, have been recognized as a relevant challenge and as an area of research interest of its own. As the number of ontologies about security grows for supporting different applications, semantic interoperability issues emerge. Relatively little attention has been paid to the ontological analysis of the concept of security understood as a broad application-independent security ontology. *Core* (or *reference*) ontologies of security cover this issue to some extent, enabling multiple applications crossing domains of security (information systems, economics, public health, crime *etc.*). In this paper, we investigate the current state-of-the-art on *Security Core Ontologies.* We select, analyze, and categorize studies on this topic, supporting a future ontological analysis of security, which could ground a well-founded security core ontology. Notably, we show that: most existing ontologies are not publicly findable/accessible; foundational ontologies are under-explored in this field of research; there seems to be no common ontology of security. From these findings, we make the case for the need of a FAIR Core Security Ontology.

Keywords: Security Core Ontology · Security Reference Ontology · Systematic mapping study · FAIR principles.

1 Introduction

Security concerns are pervasive in society across different contexts, such as economics, public health, criminology, aviation, information systems and cybersecurity, as well as international affairs. In recent years, multiple ontologies about security have been developed with the main goal of supporting different kinds of applications, such as the simulation of threats and risk management. Covering multiple application areas, *security ontologies* deal with many kinds of core and cross-domain concepts such as risk, asset, threat, and vulnerability [15]. An example of the current worries about security and, in particular, information security is the open letter addressed to the United Nation by the World Wide Web Foundation[1]. As the interest in security and related applications grows, the

[1] See https://webfoundation.org/2020/09/un-trust-and-security-letter/.

need for a rigorous analysis of the already existing resources and related concepts increases, with the main goal of enabling ontologies for information structures design and reuse. However, because of the different applications, the multiplicity of existing security ontologies dealing with different aspects of this domain brings back the issues of *semantic interoperability*, *domain understanding* and *data and model reusability*, suggesting the need for a common view, i.e., an explicit agreement about the semantics of the concepts therein. Core ontologies are intended to provide a solution to these problems, addressing to some extent the question of the general ontology of a given domain.

To better understand and organize the state-of-the-art on core ontologies of security, we carry out a systematic mapping study by following the guidelines of Petersen et al. [19]. Our contribution is a mapping of the literature about this type of ontology, selecting and categorizing the papers, then identifying research gaps. In particular, we are interested in investigating how much the existing Security Core Ontologies abide by the FAIR principles [13], i.e., how *Findable*, *Accessible*, *Interoperable* and *Reusable* are they?

This output is expected to be the basis of future research towards an ontological analysis of security, the development of a common ontology of security, and the development of an ontology-based security modeling language. The enterprise of building a general security ontology is a well-known open challenge in the field [4]. Indeed, the need for security ontology (rather than just taxonomy of security terms) was already recognized nearly two decades ago [5].

This paper is structured as follows. Section 2 establishes some definitions according to the literature; section 3 presents related work; Section 4 describes the process we followed in our mapping study; Section 5 presents the outcomes of our analysis; Section 6 briefly discuss some results; and Section 7 concludes the paper by discussing the main conclusions and prospects for future work.

2 Terminological Remarks on Ontology

The term "ontology" is semantically overloaded. In philosophy, ontology is concerned with "what there is", i.e., with the nature and characteristics of the categories of entities that are assumed to exist by some theory [20]. In Computer Science, "ontology" has several different meanings [21], but one often cited definition is that "an ontology is a formal, explicit specification of a shared conceptualisation" [26]. Obviously each term in the *definiens* requires further elaboration; for that we refer the reader to [10]. The notion of conceptualization is useful here because it allows a broader view of ontology: the things forming a conceptualization of a given domain are used to articulate abstractions of a certain state of affairs in reality [10]; a conceptualization is a sort of abstract model of some phenomenon in the world, identifying the relevant concepts and relations of that phenomenon [26]. So, a definition that is not far from the original philosophical one after all. Adopting this view, we then are going to consider ontology as whatever expresses such a conceptualization for security in a general level, regardless of the language in which this conceptualization is expressed, i.e., this might be (a) a *conceptual model*, made in a conceptual modeling language (e.g., UML) or just stated in natural language, describing the entities and relations in the domain; (b) a *formal specification* of this conceptual model (for example, in a form of a set of description logic axioms); (c) the *executable information artifact* of this specification (a *Web Ontology Language* file, for example). These three meanings are interrelated and of interest here, because we are aiming at surveying works that present core security ontologies in any of these senses.

Ontologies have different scopes or domain granularities. The broader their scope, the more generic their concepts. A *foundational ontology*, aka "upper ontology" or "top-level ontology", intends to establish a view of the most general aspect of reality, such as events, processes, identity, part-whole relation, individuation, change, dependence, causality *etc.* Examples include the Descriptive Ontology for Linguistic and Cognitive Engineering (DOLCE), the Basic Formal Ontology (BFO), and the Unified Foundational Ontology (UFO). Foundational Ontologies offer key support in the development of high-quality core and domain ontologies, improving their consistency and interoperability [9]. *Core reference ontologies* are built to grasp the central concepts and relations of a given domain, possibly integrating several domain ontologies and being applicable in multiple scenarios [21]. The terms "core ontology", "reference ontology" and "core reference ontology" or even "common ontology" often denote the same type of artifact [28]. In our context here, this kind of ontology, implicitly or explicitly, deals with the security-related concepts and relations across numerous domains of applications. Both foundational ontologies and core ontologies are application-independent, but the former are domain-independent as well.

3 Related Work

To the best of our knowledge, the first systematic literature review on security ontologies was published by Blanco et al. [3]. The authors highlight that building ontologies in the information security domain is an important research challenge. They identified that most works were focused on specific application domains, and were still at the early stages of development, lacking the available source files of the security ontologies. They concluded that the security community at that time needed yet a complete security ontology able to provide reusability, communication, and knowledge sharing. More than a decade has passed since the publication of that study, so we can verify whether some of its conclusions still hold.

A review made by Sicilia et al. [24], focused on information security ontologies that were published between 2014 and June 2015, which is a rather narrow period of analysis. Arbanas and Čubrilo [2] review and categorize information security ontologies in the same way as Blanco et al. [4]. The former covers the period between 2004 and 2014, and it does not follow a systematic methodology. The latter is a systematic literature review, more aligned with our investigation, though it was made ten years ago; [4] noticed at that time that the majority of security ontologies were focused on formalizing concrete domains to solve a specific problem.

Sikos [25] collects and describes OWL ontologies in cybersecurity, including what he calls "Upper Ontologies for Cybersecurity", which is analogous to what we call core reference security ontologies. Implementations of security ontologies in other languages were not part of that analysis.

Meriah and Rabai [16] proposes a new classification of information security ontologies: (a) ontology-based security standards and (b) ontology-based security risk assessment. The goal of their analysis is specifically to support security stakeholders choice of the appropriate ontology in the context of security compliance and risk assessment in an enterprise.

Ellerm and Morales-Trujillo [6] did a mapping study on security modeling in the context of Enterprise Architecture; they conclude there exists a necessity for reference models, security standards and regulations in the context of micromobility to enable an accurate and effective representation through modeling languages. Here, among other things, we make a case for a similar conclusion about security in a broader context (i.e., beyond micromobility).

As we see, these useful reviews have some limitations, some of which we intend to address in this work. More importantly, we notice *there is hitherto no mapping study exclusively on security core ontologies.* A reference ontology of security (in the sense discussed in Section 2 but also in the same sense of [7] for legal relations, [22] for Value and Risk, and [18] for Service) that is applicable to several security sub-domains has yet to be proposed.

4 Methodology

Our procedure is linear and follows the guidelines of Petersen et al. for systematic mapping studies in software engineering [19]:

i) **Research Questions:** We define and justify a set of input research questions, which give us the review scope, including inclusion-exclusion criteria;
ii) **Search Procedures:** We carry out the searches, defining the total amount of papers;
iii) **Screening of the Studies:** We screen them to define solely the relevant papers;
iv) **Classification Scheme:** We analyze certain parts of the relevant papers (keywords, abstract, introduction *etc.*) aiming to formulate categories for classifying the papers;
v) **Results:** We finally gather the data, then producing a landscape of reference ontologies of security - described in the results section 5.

Notice that, in this paper, when we talk about the object of our investigation, we use the terms "work", "paper", "study" and "research" interchangeably.

4.1 Research Questions

Our study is driven by the following research questions that define its scope:

RQ1: *Which security core ontologies exist in the literature?*
RQ2: *Which languages have been used to represent the core ontologies of security?*
RQ3: *Are the specifications of the security core ontologies publicly available? If so, in which source (URL)?*
RQ4: *Which foundational ontologies have been used in the design of security core ontologies?*
RQ5: *Which terms appear most often in the core ontologies of security?*

RQ2 and **RQ4** directly speaks to the topic of *interoperability* [11]; **RQ3** to *findability*; *accessibility* is indirectly assessed through findability, as the absence of the latter blocks the possibility of the former; analogously, *reusability* is indirectly assessed through *interoperoperality* and, hence, **RQ4** (with respect to the need for having rich meta-data about domain-related terms [13]) but it is also related to **RQ2**, as the use of standard languages can foster the reusability of models; **RQ1** defines the space of models of our analysis and **RQ5** the space of concepts. Through **RQ5** we also take the first steps toward a common conceptualization of the domain of security.

Given the listed RQs, we define explicit inclusion and exclusion criteria. The final collection of papers is defined by the studies that, *simultaneously*, suffice every inclusion criterion, *and* that do *not* satisfy any exclusion criteria.

Inclusion Criteria

1. Studies whose goals include introducing an ontology in at least one of the three senses we defined in section 2: conceptual models expressed in any form, formal specifications, and executable information artifacts - each describing a general conceptualization of the security domain.
2. Studies presenting a security ontology that can be seen, at least partially, as a core reference ontology, that is, an application-independent ontology describing the general concepts and relations of the domain [21], and thus, could be reused for different types of application.
3. Studies published in the last twenty years, that is, between 2000 and 2020 (included).[2]

Exclusion Criteria

1. Studies presenting application-based or microdomains ontologies of security - for example, an ontology method to solve the heterogeneity issues in a layered cloud platform [27].
2. Studies available solely in abstracts or slide presentations.
3. Publications not available in English.
4. Works about "ontological security", defined in *international relations studies* as "the need to experience oneself as a whole, continuous person in time - as being rather than constantly changing - in order to realize a sense of agency" [17].

[2] Indeed, our searches suggests there is almost no ontology-based study about security before 2000.

5. Studies on security ontology as a philosophical issue. Though they should be useful for future ontological analysis of security-related notions, our work here is focused on core ontology of security as information artifacts.

4.2 Search Procedures

Considering the RQs, in November 2020, we made several queries to the following databases, according to the search strings shown below in the exact described form: Web of Science, DBLP, ACM Digital Library, Science Direct, IEEE Xplore, Google Scholar, and Scopus. Here, the comma denotes different queries.

To formulate the search strings we assume a sort of "gold standard" based on our previous knowledge about studies that must be retrieved (such as [29], [39], [41], [50]) plus the reference of the related works (such as [4]). The goal of these search strings is to capture as many studies as possible that present some security ontology in the general level required by our scope (see especially inclusion criterion 2). At the same time, the search strings should not retrieve an overwhelming amount of papers; that is one of the reason why they are different according to the database.

Though some papers appear in multiple databases, large databases end up hiding some relevant papers because of the number of results. This is why we use different search strings in different databases: in general, we make broader searches on smaller databases, like DBLP, and we make narrower searches on bigger databases, like Google Scholar. Moreover, we have experimented and cross-checked several search string options in multiple databases before finally deciding the ones that follow.

For each database all queries were made using *the most general field of search*, except when otherwise specified. The number of results retrieved from each database and query is written with parentheses below. We used the *Harzing's Publish or Perish software*[3] to make the queries to Scopus since this software allows a convenient visualization of results. The other queries were made directly to the respective databases. Notice that in DBLP we use the term "ontolog" to capture variations like "ontological", "ontologies" and "ontology", according to the search algorithm of this database.

DBLP (263) = security ontolog (258), core reference ontology (2), common security ontology (2), security core ontology (1)

Science Direct (113) = "core security ontology" OR "security ontology" OR "core reference ontology"

[3] https://harzing.com/resources/publish-or-perish.

IEEE Xplore, ACM Digital Library (55, 67) = “core reference ontology“ OR “common security ontology” OR “security core ontology” OR “core security ontology” OR “security conceptual model” OR “security modeling language” OR “conceptual model of security” OR “core ontology of security” OR “common ontology of security” OR “general security ontology” (15, 30), “security knowledge” AND “ontology” (40, 37)

Google Scholar (591) = “common security ontology” OR “security core ontology” OR “core security ontology” OR “security conceptual model” OR “security modeling language” OR “conceptual model of security” OR “core ontology of security” OR “common ontology of security” OR “general security ontology”

Through *Harzing's Publish or Perish software*, we used the “Keywords” search (the most general search) for all queries over Scopus, except for the last two, whose searches were made over “Title words” - constrained to the periods 2010-2015 and 2016-2020.

Scopus, Web of Science (322, 294) = “core reference ontology” OR “common security ontology” OR “security core ontology” OR “core security ontology” OR “security conceptual model” OR “security modeling language” OR “conceptual model of security” OR “core ontology of security” OR “common ontology of security” (53, 160) OR “general security ontology” (4, 1) OR (“security knowledge” AND “ontology”) (63, 36) OR security ontology (202, 97)[a]

[a] We have added double quotation marks for exact phrase search in this last query on Web of Science. Otherwise more than 1400 papers are returned.

The first author was the main responsible for executing this phase, though discussion and revision were made with the other coauthors.

4.3 Screening of the Studies

The previous phase of our mapping study found thousands of papers, as seen in the last subsection. To select those relevant for us, according to the aforementioned inclusion-exclusion criteria, we proceeded to read key parts of the text as much as necessary to decide whether (or not) each study satisfies each criterion. These parts include, in the following order, the title, keywords, and abstract, and if those were not sufficient, the introduction and conclusion, and, finally, if needed, the other sections. Moreover, we compared the results of our queries to works classified as security ontology with general purpose by other reviews [4] [24] both to select relevant works and to validate our queries. During this process, we realized that some selected studies just mention ontologies of other primary studies in order to achieve their own purposes - hence, except when the former presents progress in the ontology itself, we keep only the primary study, whose main purpose was the introduction of the ontology.

This whole process was made by the first author, then the outcome was checked by co-authors of this paper, then the first author proceeded a double checking to guarantee the relevance of the selected papers according to the inclusion-exclusion criteria. After the conclusion of this phase, the amount of relevant studies was reduced to 57. They were added to “My Library” on the Google Scholar profile of the first author for storage and metadata extraction.

4.4 Classification Scheme

After this procedure, we propose the classification schemes listed below, which are related to the RQs. The classification procedure was executed by the first author, then the outcome was checked and discussed by the co-authors, then the first authors proceeded a double checking.

- **Implementation language (RQ1, RQ2):** The language used to express the ontology, in particular for execution. In case no executable implementation (like OWL) exists, we mention only the conceptual modeling language, such as *Unified Modeling Language* (UML), the logic language (say, description logic), or natural language. We also use the term “UML-like” to refer to a non-specified diagrammatic language that looks like UML class diagrams.
- **Artifact availability (RQ3):** In case the security model had been implemented, is it publicly available? If so, in which source can it be found? We have searched for the implemented model both inside the paper and on internet in general, aiming at finding the latest version of the source and of the file.
- **Foundational ontology (RQ4):** Whether or not the security ontology is based on some upper ontology, like BFO, DOLCE and UFO.
- **Concept words (RQ5):** We consider the term denoting security core concepts appearing in the selected studies, in order to describe their relative frequency. The goal is to support the identification of the most important concepts for a security common ontology.

5 Results

RQ1: Which security core ontologies exist in the literature? Our final data set of studies reporting core reference security ontologies, published between 2000 and 2020, ended up with 57 items. Their distribution in time is shown by Fig. 1. We notice there is no study published between the beginning of 2000 and the end of 2002. The list of the selected studies is attached at the end of the paper, but table. 1 already shows the collected studies presenting some security core ontology while classifying them by their representation language.

RQ2: Which languages have been used to represent the core ontologies of security? Using the data from Table 1, we plotted the pie chart shown in Fig. 2, which clearly shows the preference for OWL as the representation language of core security ontologies. This is not a surprise, considering that OWL 2 is a standard recommended by W3C since October of 2009.

RQ3: Are the specifications of the security core ontologies publicly available? If so, in which source (URL)? After searching for the file containing the ontology both within the papers and on the internet, we were only

Table 1. The 57 selected studies presenting core security ontologies grouped by their language of implementation (See RQ1, RQ2)

Language	Study
OWL	[29, 32, 41–46, 49, 50, 53, 54, 57–59, 61, 70–73, 81, 82] [34, 36–38, 52, 60, 69, 75, 77, 79, 80, 85]
UML	[40, 48, 51, 63, 65–67, 74]
Natural language	[33, 39, 55, 64, 68, 76]
UML-like	[47, 56, 83]
RDF	[35, 78]
Description Logic	[30, 62]
AS^3 Logic	[84]
XML	[31]

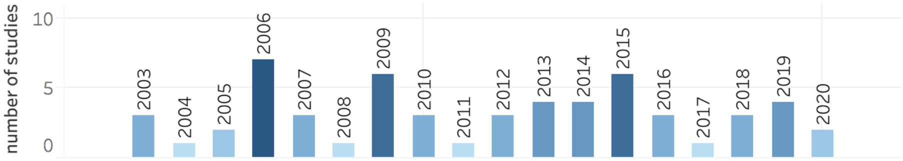

Fig. 1. 57 studies presenting core reference security ontologies grouped by year

able to find 6 of them, namely [41][4], [49][5], [53][6], [54][7], [35][8], [69][9]. We found some links, even when they were not included in their respective papers, in a dedicated catalog for security ontologies[10].

RQ4: Which foundational ontologies have been used in the design of security core ontologies? Among the 57 selected studies, only four have made use of some foundational ontology, which represents 7% of the total: [37] uses BFO, and [64, 70, 71] use DOLCE. We briefly present them below.

Massacci et al. [64] present an extended ontology for security requirements based on DOLCE that unifies concepts from the Problem Frames and Secure i* methodologies, and security concepts such as asset and threat.

Oltramari et al. [71] propose an OWL-based ontological framework that is constituted by a domain ontology of cyber operations (OSCO), which is based on DOLCE and extended with a security-related middle-level ontology (SECCO). The authors later extend this framework with the Human Factors Ontology (HUFO) [70] to support predictive cybersecurity risk assessment. Considering human factors, HUFO includes individual characteristics, situational characteristics, and relationships that influence the trust given to an individual.

[4] Source: `https://github.com/ferruciof/Files`

[5] Source: `http://semionet.rnet.ryerson.ca/ontologies/sio.owl`

[6] Source: `http://securitytoolbox.appspot.com/stac`

[7] Source: `https://www.ida.liu.se/divisions/adit/security/projects/secont/`

[8] Source: `https://sourceforge.net/projects/vulneranet/files/Wiki/`

[9] Source: `https://github.com/brunomozza/IoTSecurityOntology`

[10] `http://lov4iot.appspot.com/?p=lov4iot-security`

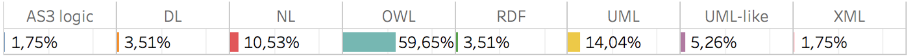

Fig. 2. Proportions of representation languages in studies shown on Table 1

Lastly, Casola et al. [37] present a "first step towards an ISO-based Information Security Domain Ontology" to support information security management systems. They show a high-level ontology for modeling complex relations among domains, and a low-level, domain-specific ontology, for modeling the ISO 27000 family of standards. To assure higher interoperability, they have made use of the principles behind BFO.

RQ5: Which terms appear most often in the core ontologies of security? Grasping the most important concepts of security is essential to devise a common ontology of security. This is the reason behind RQ5. A frequency table would be helpful to approach the issue. However, the results for RQ3 show few available files, which could be used for precise counting. To deal with that we count the frequency of the most general terms when *explicitly stated inside the ontology described in the very paper*. We also normalize some terms, for example avoiding plural, in order to reflect the frequency of the concept rather than the frequency of the word itself. The result is shown by Table 2, which shows the relative frequency of terms in the sense that it reliably presents the most common terms, though the exact counting can harmlessly vary.

Table 2. Relative frequency of most common concept terms

Concept Term	$\geqslant$ #	**Concept Term**	$\geqslant$ #
vulnerability	24	risk	9
asset	23	attacker	7
threat	21	control	7
countermeasure	12	stakeholder	6
attack	9	consequence	6

Among the 57 selected studies, each work presents a security ontology and each term appears only once in each ontology if it appears at all. Then we can conclude there exists no concept shared by all selected ontologies. This suggests a general lack of agreement between those security ontologies. At this point, we may wonder whether some of the selected ontologies have been more adopted than others. Since the number of citations (in Google Scholar) offers an approach to this question, we notice [33] with more than 6500 citations stands out from any other work. Studies with the number of citations between 100 up to 300 citations are [39, 46, 50, 54, 58, 65, 80].

6 The Need for a FAIR Core Security Ontology

The interest in security ontologies has been growing in the last fifteen years. Most likely because of the rapid growth of Web apps and the popularization of the internet, which remarkably increased information security concerns. However, these ontologies are not easily *findable* since only circa 10% of them are publicly available. Indeed, the lack of availability of security ontologies was noted by [3] in 2008, so this scenario has not changed signifcantly so far.

Moreover, the use of foundational ontologies for grounding core security ontologies is still very incipient. The lack of a foundational ontology supporting the construction of a domain ontology is not a problem *per se*. However, studies have shown that foundational ontologies significantly contribute to prevent and to detect bad ontology design [23], improving the quality and interoperability of domain and core ontologies [14]. Indeed, modeling domain and core ontologies without making explicit the underlying ontological commitments of the conceptualization gives rise to semantic interoperability problems. In fact, there is a strong connection between the ability of articulating domain-specific notions in terms of formal ontological categories in conceptual models, and the *interoperability* of these artifacts [11].

Semantic interoperability is also hindered by the sole use of languages such as OWL, which merely address logical issues neglecting truly ontological ones [9,11]. Once meaning negotiation and semantic interoperability issues have been established by the usage of an ontologically well-founded modeling language, knowledge representation languages such as OWL can be employed for ontology implementation if necessary [9].

Still regarding interoperability, in our set of selected papers, only four ontologies grounded on a foundational ontology were identified, three of which are based on DOLCE. As demonstrated in [22], risk (and, hence, risk management, including risk control measures) is an inherently relational phenomenon. This makes DOLCE an odd choice for grounding a reference ontology in this area, given that it does not support relational aspects (relational qualities and bundles thereof) (see [12]). In contrast, UFO comprises a rich theory of relations that has successfully been used to address related phenomena such as risk, value [22], and trust [1].

In assessing *reusability*, we focus here on two aspects, namely, whether the ontologies *meet domain-relevant community standards* and whether they they *provide rich metadata* [13]. Regarding the former, one positive aspect is the fact that most of the ontologies found in our study are represented using international standard languages (e.g., OWL - which is a W3C standard - and UML - which is a OMG *de facto* standard - together account for 73,69% of all the models as per figure 1). This at least affords syntactic reusability as well as some predictability in terms of automated inference (in the case of OWL models). However, from a semantic point of view, reusability requires a safe interpretation of the elements being reused in terms of the correct domain categories. In this sense, rich metadata grounded in well-understood ontological categories is as important for safe reusability as it is for safe interoperability. Here, the same limitations identified for the latter (e.g., the use of ontologically-poor languages such as OWL and UML [9], and the lack of use of foundational ontologies) can also be identified as a hindrance to the former.

In summary, our study highlights the need for advancing on the proposal of Core Security Ontologies that are *Findable, Accessible, Interoperable and Reusable, i.e., FAIR* [13].

7 Conclusion

In this paper, we presented a systematic mapping study about the literature on core reference security ontologies, considering the last twenty years of research. We started an analysis to understand this research scenario, the implementation languages that have been used, the availability of the ontology files, the domains, and the role of foundational ontologies in security ontologies. Our mapping study has made clear an important research gap in security ontology field: there seems to be no domain-independent core security ontology in the same general sense of [7] for Legal Relations, [22] for Value and Risk, and [18] for Service. Moreover, foundational ontologies are very underutilized in the field (interoperability). Another gap is the lack of public availability of the actual security core ontologies as artifacts (findability), which makes their analysis and (re)use difficult.

As future work, we intend to use the results of this systematic review as support for the development of a well-founded security ontology grounded on the Unified Foundation Ontology [8] and as an extension of the Common Ontology of Value and Risk [22], following *FAIR* principles [13].

Acknowledgement

This work is supported by Accenture Israel Cyber R&D Lab. (*RiskGraph* project).

References

1. Amaral, G., et al.: Towards a reference ontology of trust. In: Intl. Conf. on Cooperative Information Systems. vol. 11877, pp. 3–21 (2019)
2. Arbanas et al, Information and Organizational Sciences **39**(2), 107–136 (2015)
3. Blanco et al: A systematic review and comparison of security ontologies. In: 3rd Intl. Conf. Availability, Reliability and Security. pp. 813–820. Ieee (2008)
4. Blanco et al: Basis for an integrated security ontology according to a systematic review of existing proposals. Computer Standards & Interfaces **33**(4) (2011)
5. Donner, M.: Toward a security ontology. IEEE Security & Privacy (3), 6–7 (2003)
6. Ellerm et al: Modelling security aspects with archimate: A systematic mapping study. In: Euromicro Conf. on Software Engineering and Advanced Applications. pp. 577–584. IEEE (2020)
7. Griffo, C.: Ufo-l: A core ontology of legal concepts built from a legal relations perspective. Doctoral Consortium Contributions, IC3K-KEOD (2015)
8. Guizzardi, G.: Ontological foundations for structural conceptual models. CTIT, Centre for Telematics and Information Technology (2005)
9. Guizzardi, G.: The role of foundational ontologies for conceptual modeling and domain ontology representation. In: 2006 7th International Baltic Conf. on databases and information systems. pp. 17–25. IEEE (2006)

10. Guizzardi, G.: On ontology, ontologies, conceptualizations, modeling languages, and (meta) models. Frontiers in artificial intelligence and applications **155**, 18 (2007)
11. Guizzardi, G.: Ontology, ontologies and the "I" of FAIR. Data Intelligence **2**(1-2), 181–191 (2020)
12. Guizzardi et al: Towards ontological foundations for conceptual modeling: The unified foundational ontology (ufo) story. Applied ontology **10**(3-4), 259–271 (2015)
13. Jacobsen, A., et al.: FAIR principles: interpretations and implementation considerations. Data Intelligence **2**(1-2), 10–29 (2020)
14. Keet, C.M.: The use of foundational ontologies in ontology development: an empirical assessment. In: ESWC. pp. 321–335. Springer (2011)
15. Kovalenko et al: Knowledge model and ontology for security services. In: Intl. Conf. on System Analysis & Intelligent Computing. pp. 1–4. IEEE (2018)
16. Meriah et al: Analysing information security risk ontologies. International Journal of Systems and Software Security and Protection **11**(1), 1–16 (2020)
17. Mitzen, J.: Ontological security in world politics: State identity and the security dilemma. European journal of international relations **12**(3), 341–370 (2006)
18. Nardi et al: A commitment-based reference ontology for services. Information systems **54**, 263–288 (2015)
19. Petersen et al: Systematic mapping studies in software engineering. In: 12th Intl. Conf. Evaluation and Assessment in Soft. Engineering (EASE) 12. pp. 1–10 (2008)
20. Quine, W.V.: On what there is. The review of metaphysics pp. 21–38 (1948)
21. Roussey et al: An introduction to ontologies and ontology engineering. In: Ontologies in Urban development projects, pp. 9–38. Springer (2011)
22. Sales et al: The common ontology of value and risk. In: Intl. Conf. on Conceptual Modeling. pp. 121–135. Springer (2018)
23. Schulz, S.: The role of foundational ontologies for preventing bad ontology design. In: 4th Joint Ontology Workshops (JOWO). vol. 2205. CEUR-WS (2018)
24. Sicilia et al: What are information security ontologies useful for? In: Research Conf. on Metadata and Semantics Research. pp. 51–61. Springer (2015)
25. Sikos, L.F.: OWL ontologies in cybersecurity: conceptual modeling of cyber-knowledge. In: AI in Cybersecurity, pp. 1–17. Springer (2019)
26. Studer et al: Knowledge engineering: principles and methods. Data & knowledge engineering **25**(1-2), 161–197 (1998)
27. Tao et al: Multi-layer cloud architectural model and ontology-based security service framework for iot-based smart homes. Future Generation Computer Systems **78**, 1040–1051 (2018)
28. Zemmouchi-Ghomari et al: Reference ontology. In: Int. Conf. on Signal Image Technology and Internet Based Systems. pp. 485–491. IEEE (2009)

Selected Studies

29. Agrawal, V.: Towards the ontology of ISO/IEC 27005: 2011 risk management standard. In: Intl. Symp. on Human Aspects of Information Security & Assurance. pp. 101–111 (2016)
30. do Amaral, F.N., et al.: An ontology-based approach to the formalization of information security policies. In: Intl. Enterprise Distributed Object Computing Conf. Ws. IEEE (2006)
31. An Wang et al: An ontological approach to computer system security. Information Security Journal: A Global Perspective **19**(2), 61–73 (2010)

32. Arogundade et al: Towards an ontological approach to information system security and safety requirement modeling and reuse. Information Security Journal: A Global Perspective **21**(3), 137–149 (2012)
33. Avizienis et al: Basic concepts and taxonomy of dependable and secure computing. IEEE transactions on dependable and secure computing **1**(1), 11–33 (2004)
34. Beji et al: Security ontology proposal for mobile applications. In: 10th Intl. Conf. Mobile Data Management: Systems, Services and Middleware. IEEE (2009)
35. Blanco, F.J., et al.: Vulnerapedia: Security knowledge management with an ontology. In: Intl. Conf. on Agents and Artificial Intelligence. pp. 485–490 (2012)
36. Boualem et al: Maintenance & information security ontology. In: Intl. Conf. on Control, Decision and Information Technologies. pp. 312–317. IEEE (2017)
37. Casola et al: A first step towards an iso-based information security domain ontology. In: Intl. Conf. on Enabling Technologies: Infrastructure for Collaborative Enterprises. pp. 334–339. IEEE (2019)
38. Chen et al: Research on ontology-based network security knowledge map. In: Intl. Conf. on Cloud Computing, Big Data and Blockchain. pp. 1–7. IEEE (2018)
39. Cherdantseva et al: A reference model of information assurance & security. In: Intl Conf on Availability, Reliability and Security. pp. 546–555. IEEE (2013)
40. Chowdhury, M.J.M.: Security risk modelling using secureuml. In: 16th Int'l Conf. Computer and Information Technology. pp. 420–425. IEEE (2014)
41. de Franco Rosa et al: Towards an ontology of security assessment: A core model proposal. In: Information Technology-New Generations, pp. 75–80. Springer (2018)
42. Dos Santos Moreira et al: Ontologies for information security management and governance. Information Management & Computer Security (2008)
43. Dritsas et al: Employing ontologies for the development of security critical applications. In: Challenges of Expanding Internet: E-Commerce, E-Business, and E-Government, pp. 187–201. Springer (2005)
44. Ekelhart et al: Ontology-based business knowledge for simulating threats to corporate assets. In: Int. Conf. on Practical Aspects of Knowledge Management. pp. 37–48. Springer (2006)
45. Ekelhart et al: Security ontology: Simulating threats to corporate assets. In: Intl. Conf. on Information Systems Security. Springer (2006)
46. Ekelhart et al: Security ontologies: Improving quantitative risk analysis. In: Annual Hawaii Intl. Conf. on System Sciences. pp. 156a–156a. IEEE (2007)
47. El-Attar et al: Extending the uml statecharts notation to model security aspects. IEEE Transactions on Software Engineering **41**(7), 661–690 (2015)
48. Elahi et al: A modeling ontology for integrating vulnerabilities into security requirements conceptual foundations. In: Intl. Conf. on Conceptual Modeling. pp. 99–114. Springer (2009)
49. Fani et al: An ontology for describing security events. In: SEKE. pp. 455–460 (2015)
50. Fenz, S., et al.: Formalizing information security knowledge. In: Intl. Symp. on Information, Computer, and Communications Security. pp. 183–194 (2009)
51. Fernandez et al: A security reference architecture for cloud systems. In: WICSA 2014 Companion Volume, pp. 1–5 (2014)
52. Guan et al: An ontology-based approach to security pattern selection. Intl. J. of Automation and Computing **13**(2), 168–182 (2016)
53. Gyrard, A., et al.: The STAC (security toolbox: attacks & countermeasures) ontology. In: Intl. Conf. on World Wide Web. pp. 165–166 (2013)
54. Herzog et al: An ontology of information security. Intl. J. of Information Security and Privacy **1**(4), 1–23 (2007)

55. Jonsson, E.: Towards an integrated conceptual model of security and dependability. In: Intl. Conf. on Availability, Reliability and Security. IEEE (2006)
56. Kang et al: A security ontology with MDA for software development. In: Intl. Conf. on Cyber-Enabled Distributed Computing and Knowledge Discovery. pp. 67–74 (2013)
57. Karyda et al: An ontology for secure e-government applications. In: Intl. Conf. on Availability, Reliability and Security. pp. 5–pp. IEEE (2006)
58. Kim, A., et al.: Security ontology for annotating resources. In: Int. Conf. on Ontologies, Databases and Applications of Semantics. pp. 1483–1499. Springer (2005)
59. Kim et al: Analytical study of cognitive layered approach for understanding security requirements using problem domain ontology. In: Asia-Pacific Software Engineering Conference. pp. 97–104. IEEE (2016)
60. Kim et al: Understanding and recommending security requirements from problem domain ontology: A cognitive three-layered approach. Journal of Systems and Software **169**, 110695 (2020)
61. Korger, A., Baumeister, J.: The SECCO ontology for the retrieval and generation of security concepts. In: Case-Based Reasoning Research and Development (2018)
62. Li et al: An ontology-based learning approach for automatically classifying security requirements. Journal of Systems and Software p. 110566 (2020)
63. Lund et al: UML profile for security assessment. Tech.Report STF A **3066** (2003)
64. Massacci et al: An extended ontology for security requirements. In: Intl. Conf. on Advanced Information Systems Engineering. pp. 622–636. Springer (2011)
65. Mayer, N.: Model-based management of information system security risk. Ph.D. thesis, University of Namur (2009)
66. Mayer et al: An integrated conceptual model for information system security risk management supported by enterprise architecture management. Software & Systems Modeling **18**(3), 2285–2312 (2019)
67. Milicevic et al: Ontology-based evaluation of iso 27001. In: Conference on e-Business, e-Services and e-Society. pp. 93–102. Springer (2010)
68. Mouratidis, H., et al.: An ontology for modelling security: The Tropos approach. In: Intl. Conf. on Knowledge-Based and Intelligent Information and Engineering Systems. pp. 1387–1394. Springer (2003)
69. Mozzaquatro, B.A., et al.: Towards a reference ontology for security in the internet of things. In: Intl Work. on Measurements & Networking. pp. 1–6. IEEE (2015)
70. Oltramari, A., et al.: Towards a human factors ontology for cyber security.
71. Oltramari, A., et al.: Building an ontology of cyber security. In: Conf. on Semantic Technology for Intelligence, Defense, and Security. vol. 1304, pp. 54–61 (2014)
72. Parkin, S.E., et al.: An information security ontology incorporating human-behavioural implications. In: Proceedings of SIN'09. pp. 46–55 (2009)
73. Pereira et al: An ontology approach in designing security information systems to support organizational security risk knowledge. In: KEOD. pp. 461–466 (2012)
74. Pereira et al: A stamp-based ontology approach to support safety and security analyses. Journal of Information Security and Applications **47**, 302–319 (2019)
75. Ramanauskaitė et al: Security ontology for adaptive mapping of security standards. Intl. J. Computers, Communications & Control **8**(6), 813–825 (2013)
76. Schumacher, M.: Toward a security core ontology. In: Security engineering with patterns, pp. 87–96. Springer (2003)
77. Souag et al: A security ontology for security requirements elicitation. In: Intl. Symp. Engineering secure software and systems. pp. 157–177. Springer (2015)
78. Takahashi et al: Reference ontology for cybersecurity operational information. The Computer Journal **58**(10), 2297–2312 (2015)

79. Tsoumas et al: Security-by-ontology: A knowledge-centric approach. In: IFIP International Information Security Conference. pp. 99–110. Springer (2006)
80. Tsoumas et al: Towards an ontology-based security management. In: Intl. Conf. on Advanced Information Networking and Applications. vol. 1, pp. 985–992 (2006)
81. Vale et al: An ontology for security patterns. In: 38th Int. Conf. of the Chilean Computer Science Society. pp. 1–8. IEEE (2019)
82. Vorobiev, A., Bekmamedova, N.: An ontological approach applied to information security and trust. Australasian Conf. on Information Systems p. 114 (2007)
83. Vorobiev et al: An ontology-driven approach applied to information security. Journal of Research and Practice in Information Technology **42**(1), 61 (2010)
84. Yau et al: An adaptable distributed trust management framework for large-scale secure service-based systems. Computing **96**(10), 925–949 (2014)
85. Zheng-qiu et al: Semantic security policy for web service. In: Int. Symp. Parallel and Distributed Processing with Applications. pp. 258–262. IEEE (2009)