UDC 004.822:004.056
Original Scientific Paper

Ontology in Information Security

Krunoslav Arbanas *karbanas@foi.hr*
Paying Agency for Agriculture, Fisheries and Rural Development
Zagreb, Croatia

Mirko Čubrilo *mcubrilo@foi.hr*
Faculty of Organization and Informatics
University of Zagreb, Varaždin, Croatia

Abstract

The past several years we have witnessed that information has become the most precious asset, while protection and security of information is becoming an ever greater challenge due to the large amount of knowledge necessary for organizations to successfully withstand external threats and attacks. This knowledge collected from the domain of information security can be formally described by security ontologies. A large number of researchers during the last decade have dealt with this issue, and in this paper we have tried to identify, analyze and systematize the relevant papers published in scientific journals indexed in selected scientific databases, in period from 2004 to 2014. This paper gives a review of literature in the field of information security ontology and identifies a total of 52 papers systematized in three groups: general security ontologies (12 papers), specific security ontologies (32 papers) and theoretical works (8 papers). The papers were of different quality and level of detail and varied from presentations of simple conceptual ideas to sophisticated frameworks based on ontology.

Keywords: information, security, ontology, security ontology, knowledge formalization

1. Introduction

Over the years, information technology (IT) has penetrated into every aspect of modern business organizations critically dependent on its production, processing, transmission and storage of today's key resource - information. This fact has led to an evolution of the role of information security, which has long been seen exclusively as a technical issue and an integral part of IT department [54]. However, the awareness is gradually growing that information security is not just a technical issue [58] but a responsibility of corporate governance that includes risk management, controls reporting, testing, training and management responsibilities [66], [11].

Since the top management is responsible for results and continuity of the organization, their biggest task is to identify the right questions about security issues and take them into account in the overall management of IT infrastructure and services. Information security requires a holistic, systematic and comprehensive approach i.e. the framework for information security governance, which enables an organization to consider information security not only at a technical level but also as an important part of the overall strategic planning [36], [58].

Based on the decision-making structure of information systems, information security governance framework is organized on three levels: the operational, the tactical and the strategic level. *The operational level* describes the everyday, common and reactive activities necessary to maintain business delivery capabilities by the IT infrastructure. At this level, there is a large amount of data with low strategic importance. *The tactical level* provides information obtained by data analysis from operational level and defines a set of proactive

activities for quality IT service delivery. The *strategic level* is essential for better understanding governance's role and its structure organization at the high level of information security. At this level, there is a small amount of information, but of critical importance [36],[58].

Together with the development of IT-enabled business operations, management and decision-making in the networked market conditions, the dimension of knowledge and information has become critical in today's business organizations. Business management is faced with challenges of taking into account different types of information from different sources. It is generally accepted that the information is an asset which is, like other important business resources, essential for the organization and, consequently, its appropriate protection is necessary. In general, security is dealing with the issue of protection of assets from threats, where threats are categorized as potential for assets' misuse. Protecting and maintaining the organization's integrity is particularly important for knowledge and unique and critical skills and resources owned by the organization [1].

In addition to the need for implementation of information security measures in almost any environment and coping with a growing range of applications, mutual understanding and use of precisely defined terminology is becoming increasingly difficult for professionals from different areas, [19] and even 10 years ago it was said that too much security terminology is vaguely defined, making it difficult to communicate between colleagues and, even worse, confusing for those who need to use it [53]. However, as decision-making process has become a central and strategic advantage, the organization's success increasingly depends on its ability to produce, collect, store, manage and disseminate knowledge [36].

Since the awareness of knowledge in security field has increased in scientific community, during the last decade many models of this knowledge formalization are proposed in form of security ontologies. But the question is, how can ontologies be used for information security purposes, what types of security ontologies exist, what do they cover and how many authors have dealt with this subject?

Based on the questions stated above, the goal of this paper is to review, analyze, select and classify security ontologies based on relevant literature published between 2004 and 2014. Based on the analysis of titles, keywords, summary and conclusion, relevant papers regarding security ontologies will be selected and grouped into three groups: general security ontologies, specific security ontologies and theoretical works, as proposed by Blanco et al. [7]. Thus, this paper represents a sort of extension of that paper as it covers the analysis of new concepts related to security ontologies.

2. Ontology and Information Security

Information as a key asset of an organization is valuable, but at the same time also sensitive, since through its lifecycle information can be intercepted, modified, terminated, invented or destroyed [65]. Therefore, as stated in international standard ISO/IEC 27002, information security is "*the protection of information from wide range of threats in order to ensure business continuity, minimize business risk and maximize return on investments and business opportunities*" [25]. At the same time, with increasing security levels of this information, established information security achieves an additional amount of information, which makes information manipulation and management more difficult. Due to a large volume of information obtained from various sources, such as system records, firewall logs or vulnerability warnings, security administrators are faced with difficult problem of effective knowledge generation about information security problems, warnings and incidents they are faced with and need to make right decisions [34].

Most of these decisions are made based on administrator's tacit knowledge, which leads to a recognition of importance for facilitating automatic correlation of various security incidents and vulnerabilities coming from different sources, as well as security and knowledge management which enables development of security incident and vulnerability ontologies that define unique concept and relation vocabulary related to these [36].

Information security, as direct responsibility for corporate governance that lies on the shoulders of organization's management [58], becomes a critical success factor and helps organizations in transforming today's threats in tomorrow's possibilities for achieving competitive advantage [54] by protecting information assets from loss, operational discontinuity, abuse, unauthorized access, inaccessibility and damage [26]. Also, information security is an important aspect of the development of information systems as well as for organizations' survival while security community manages many concepts and relationships that need to be supported by ontologies. Information security has undergone a major evolution in the scientific community and the number of events and journals focused on security has increased dramatically, which means that it is currently one of the most thriving scientific disciplines. Therefore, the existence of an ontology that clearly defines, classifies and links related concepts is very important [7].

In information and computer science, knowledge is represented in a variety of ways, ranging from large amounts of databases, collections of documents and e-mails to explicit schemes and structures, Internet connections, folder hierarchies or business process descriptions. In addition to this, the fact that computing resources are becoming cheaper increases the so-called "information flood". The ways are sought to take advantage of this overall knowledge and not just individual elements of information. Since the beginning of computer systems, integration of information has always been one of the most important topics as most of the existing knowledge representation is not yet compatible with each other [13]. On the other hand, ontological paradigm aims to support the sharing and reuse of knowledge in an explicit and mutually agreed way [56].

For the lion's share of information the question is how to manage the data collection related to the vulnerability of information systems in a way that different managers can access and understand it without misinterpretation of their meaning. This question arises because, for example, the same software vulnerabilities can be published under different names (or codes) and descriptions of various security organizations (CERT, ISO, NIST, etc.) or various software companies. The same can happen with, e.g., security controls and corrective measures [36].

Often wrong decisions are made due to the lack of knowledge about the security domain, threats, potential countermeasures and assets of the organization. There are several reasons for this. First, security terminology for many concepts is not well defined, leading to confusion among security professionals and users [52],[22], and also, decisions about security organizations are made by managers who do not fully understand the full depth of the underlying IT infrastructure. Such ambiguity can be mitigated by common repository of domain knowledge in security domain [22] where security ontologies provide a precise definition of entities and their relationships [52], or in other words, ensure a common and accurate terminology [22]. Ontology is a simplified summarized view of reality that represents knowledge in a formal and structured format and provides better communication, reusability and knowledge organization, as well as basis for high level reasoning and decision-making [7], [65].

2.1. Term *Ontology*

The word *ontology* comes from the Greek words *ontos* (being) and *logos* (word) and it was introduced in the philosophy in the 19th century by German philosophers to distinguish such type of study from the study of various types of existence in natural sciences [10].

Currently, there are different definitions in the literature of what ontology should be and there is no universal definition of ontology, which is one of the reasons for the wide range of its possible applications.

The definition of ontology often quoted in semantic Web literature, and which is also considered to be most appropriate by the authors of this paper, is the one made by Gruber in 1993 [10], [13], [38]: "An ontology is a formal, explicit specification of a conceptualization of common areas of interest". *Conceptualization* represents an abstract model; *explicit* means that the elements must be clearly defined; and *formal* indicates that the specification should be

machine-readable (processable) [10]. *Shared* reflects the notion that an ontology captures consensual knowledge, i.e., not only for the individual. *Common* does not necessarily mean that it is globally shared but accepted by a group. Finally, reference to *an area of interest* shows that with the domain ontologies one is not interested in modeling the entire world, but for modelling only those parts of a particular domain relevant to his/her task [13], [38].

So, we can say that ontology is a specification of concepts and their relationships which represents knowledge in a formal and structured format and provides a better tool for communication, reusability and organization of knowledge. Ontology provides a possibility of formal logic reasoning on the basis of well-defined data and knowledge bases, records the relationships between collected data and uses explicit knowledge of concepts and relationships for reasoning about implicit and inherent knowledge, while ontology alignment, in terms of identifying relationships between individual elements of multiple ontologies, is a necessary prerequisite for establishing interoperability between agents or services using different ontologies [13].

A special kind of ontology is a *taxonomy* that classifies concepts hierarchically, using superior and subordinate relationship (father-son, part-of or type-of) [10]. This means that, while ontologies can have any type of relationship between categories (part-in, cause-effect, association, etc.), in taxonomy there can only be a generalization hierarchy [53]. Furthermore, taxonomy does not allow you to specify attributes for terms, which means that, if you need any of these features, you must resort to ontologies [10].

The ontology defines a common vocabulary for researchers who need to share information within a domain. It includes machine interpretative definitions of basic concepts within a domain and relationships among them. Some of the reasons for ontology development are: possibility of sharing a common understanding of information structure among either people or software agents; making domain knowledge reusable; explicitness of domain assumptions; separation of domain and operational knowledge and analysis of domain knowledge [39].

Main components which constitute an ontology are: *concepts (classes), relationships, axioms, properties (attributes)* and *instances*. *Concepts* are abstract terms, usually organized in taxonomies, that can have *properties* (or *attributes*), which help in establishing a relationship between non-hierarchical concepts that describe the common characteristics of class instances or class relations, and can have certain type (e.g. STRING, INTEGER, BOOLEAN, etc.). *Axioms* are rules that apply in modeled domain and limit the possible interpretations of defined concepts. Ontologies provide inheritance in an object-oriented way, where *instances* represent the actual occurrence of abstract concepts [37], [56].

Ontologies are used in various areas of computer science (such as (among others), artificial intelligence, knowledge representation, natural language processing, semantic web and software engineering) in order to facilitate the exchange of knowledge and its reuse [10].

2.2. Security Ontologies

In general, in information systems ontologies are mainly used to obtain information and knowledge representation, sharing and management [38], while ontologies applied to information security can be roughly divided into general security ontologies that include all (or most) of the security concepts [53] and specific security ontologies related to the individual part of information security domain.

The goal of security ontologies is to create common, unambiguous semantic models of security domain concepts that will serve as a basis for communication between people or software agents which leads to a reduction of language ambiguity, while at the same time providing a means for easy expansion and usefulness in research projects [9], [7].

There are several papers [53], [8], [7], [38] in which authors have reviewed relevant papers on the topics of proposed security ontologies and their application.

2.2.1. *Ontologies for Security Requirements: A Literature Survey and Classification*

Souag et al. [53] made a review of relevant and known literature sources looking for articles related to ontologies, requirements, security and its different aspects. Based on the results, they suggested classification of security ontology which consists of eight groups consisting of: initial security ontologies, security taxonomies, general security ontologies, specific security ontologies, security risk-based ontologies, Web-oriented security ontologies, security requirements ontologies, modeling security ontologies. In some cases, security ontologies simultaneously belong to two categories and, in these cases, ontology has been assigned to the dominant research area. This research showed the existence of significant number of papers about security ontologies and also showed that the existing security ontologies differ considerably in the way they cover security aspects. The authors have tried to analyze how each ontology covers certain security aspects and to investigate whether the proposed ontologies can be used to define security requirements and to what extent. The results revealed a gap between security requirements engineering and ontology areas, and thus a new field of research [53].

2.2.2. *A Systematic Review and Comparison of Security Ontologies*

Blanco et al. [8] are using the method of the systematic literature review to identify and analyze existing proposals in ontological engineering applied to information security field. The Authors did a literature review by taking into account scientific databases ScienceDirect, ACM digital library, IEEE digital library, Google Scholar and DBLP as data sources. They took into account only papers are written in English and the criteria for selecting individual papers were focused on the analysis of titles, keywords and abstracts of analyzed papers. Based on this research, the authors have classified papers in three groups: security ontologies (general and applied to specific area) with a total of 17 papers, theoretical works (4 papers) and semantic web-oriented works (9 papers).

2.2.3. *Basis for an integrated security ontology according to a systematic review of existing proposals*

The result of extended systematic literature review [7] conducted by same authors, which included a review, an analysis and a comparison of security ontologies proposals, was the identification of initiatives related to security ontologies. The aim was to find and classify research according to its purpose, which can be: defining general purpose security ontologies, defining security ontologies focused on particular domain or defining theoretical works which, despite their interesting contributions, do not formally define an ontology. Based on this criterion, the focus was on the analysis of titles, keywords, and paper abstracts in order to discover relationships between ontological engineering concepts applied to the security area. In doing this, the authors discovered relevant proposals and separated them from research irrelevant to the topic. Security standards were not considered as security ontologies because they represent pure concepts and taxonomies used in making of these ontologies. The results consisted of 8 general security ontologies, 20 specific security ontologies, and 3 theoretical works. As a conclusion of this study, authors have found out that although these security ontologies make an important contribution to the security community, they offer only partial solutions for incorporating their knowledge into an integrated security ontology. Moreover, it has been found out that a successful implementation of this overall integrated ontology is a difficult and complex task that requires extensive discussion and consensus within the scientific and professional community [7].

2.2.4. *Ontologies and Information Systems: A Literature Survey*

In his paper [38] Nguyen gives a basic overview of ontology-related researches and developments, and their application to information systems. The primary objective of this

study is to help discover areas of interest and conduct further literature research. For this purpose (in addition to information about ontologies in general), the article also includes some specific comments on the use of ontologies in computer networks modeling and security.

2.3. Use of ontologies in information security: literature review

The aim of this paper is to review, analyze, select and classify security ontologies on the basis of relevant literature. The search for relevant publications was conducted within the scientific databases ScienceDirect, ACM digital library, IEEE digital library and Google Scholar by searching for the titles of papers published in the period from 2004 to 2014 according to the query: (ontology AND security) OR ("Ontological Engineering" AND security) OR (ontology AND privacy) OR "security ontology".

Based on analysis of titles, keywords, abstracts and conclusions, relevant papers dealing with the topic of security ontologies were selected and roughly grouped into three groups that consist of general security ontologies, specific security ontologies and theoretical works, as proposed by Blanco et al. [8]. The research results are grouped in Table 1.

No.	Ontology proposals	General security ontology	Specific domain of security ontology	Theoretical works
1.	A Bootstrapping Approach for Developing a Cyber-Security Ontology Using Textbook Index Terms	X		
2.	A Modeling Ontology for Integrating Vulnerabilities into Security Requirements Conceptual Foundations		Security requirements	
3.	A Qualitative Analysis of An Ontology Based Issue Resolution System for Cyber Attack Management		Security attacks	
4.	A Security Audit Framework to Manage Information System Security			X
5.	A Security Framework for Audit and Manage Information System Security			X
6.	A Security Ontology for Incident Analysis		Security incidents	
7.	A Security Ontology with MDA for Software Development		Software development	
8.	A Semantic-based Intrusion Detection Framework for Wireless Sensor Network		Network security	
9.	A Study on Security and Ontology in Cloud Computing		Cloud computing	
10.	A user-oriented ontology-based approach for network intrusion detection		Network security	
11.	An Efficient Network Security System through an Ontology Approach		Network security	
12.	An Extended Ontology for Security Requirements		Security requirements	
13.	An Information Security Ontology Incorporating Human-Behavioral Implications		Human factor	
14.	An Ontological Approach Applied to Information Security and Trust	X		
15.	An Ontological Approach to Information Security Education		Information security education	
16.	An Ontology Based Approach to Information Security			X
17.	An Ontology-Based Approach to Information Systems Security Management			X
18.	An Ontology-based Approach to the Formalization of Information Security	X		

No.	Ontology proposals	General security ontology	Specific domain of security ontology	Theoretical works
	Policies			
19.	An Ontology of Information Security	X		
20.	An Ontology for Network Security Attacks		Network security	
21.	An ontology for secure e-government applications		Security requirements	
22.	An Ontology Framework for Managing Security Attacks and Defences in Component Based Software Systems		Security attacks	
23.	An Ontology-Driven Approach Applied to Information Security	X		
24.	An OWL-based Security Incident Ontology		Security incidents	
25.	Application of Security Ontology to Context-Aware Alert Analysis		Network security	
26.	Constructing Enterprise Information Network Security		Network security	
27.	Data Center Physical Security Ontology for Automated Evaluation		Physical security	
28.	Developing an Ontology of the Cyber Security Domain			X
29.	Formalizing Information Security Knowledge	X		
30.	Ontological Approach toward Cyber security in Cloud Computing		Cloud computing	
31.	Ontological Mapping of Information Security Best-Practice Guidelines	X		
32.	Ontologies for information security management and governance	X		
33.	Ontologies for Modeling Enterprise Level Security Metrics	X		
34.	Ontology Based Approach for Perception of Network Security State		Network security	
35.	Ontology based IT-security planning	X		
36.	Ontology Development for Business Impact Analysis in Information Technology Business Continuity Management for Public Sector in Malaysia		Business Impact Analysis	
37.	Ontology for attack detection: An intelligent approach to web application security		Web application security	
38.	Ontology for Detection of Web Attacks		Network security	
39.	Ontology-Based Model of Network and Computer Attacks for Security Assessment		Network security	
40.	Ontology-Based Security Standards Mapping Optimization by the Means of Graph Theory			X
41.	OVM: An Ontology for Vulnerability Management		Vulnerabilities	
42.	Security Attack Ontology for Web Services		Web services attacks	
43.	Security Data Mining in an Ontology for Vulnerability Management		Vulnerabilities	
44.	Security Ontologies: Improving Quantitative Risk Analysis	X		
45.	Security Ontology Construction and Integration			X
46.	Security Ontology for Adaptive Mapping of Security Standards		Security standards	
47.	Security ontology proposal for mobile		Mobile applications	

No.	Ontology proposals	General security ontology	Specific domain of security ontology	Theoretical works
	applications			
48.	The Design, Instantiation, and Usage of Information Security Measuring Ontology		Information security metrics	
49.	The STAC (Security Toolbox: Attacks & Countermeasures) Ontology	X		
50.	Toward a Unified Ontology of Cloud Computing		Cloud computing	
51.	Towards an Ontology for Cloud Security Obligations		Cloud computing	
52.	Towards an Ontology-based Security Management			X
	TOTAL	**12**	**32**	**8**

Table 1. Summary of security ontologies. Source: authors' representation

Below is a brief overview of basic features of analyzed papers.

A Bootstrapping Approach for Developing a Cyber-Security Ontology Using Textbook Index Terms [63]

In this paper authors proposed a bootstrapping method for cyber security ontology development using existing security ontology as a foundation and security textbooks index that gives a list of terms in the security domain. The bootstrapping approach automatically extracts terms and concepts from textbooks' index, derives relationship according to the concept from security ontology for each term and classifies them into existing security ontology. This approach relies on exact and approximate matching concepts similarities, as well as on category information obtained from external sources, e.g. Wikipedia. Results showed validity of this method for development of comprehensive and scalable cyber security ontology, enriched with concepts from textbooks' index, which can be used for recording and searching for learning materials, education and training in cyber security field.

A Modeling Ontology for Integrating Vulnerabilities into Security Requirements Conceptual Foundations [15]

This paper proposes a modeling ontology focused on vulnerabilities, which aims to integrate empirical knowledge about vulnerabilities into system development process. Based on literature review, authors identified basic concepts for modeling and analysis of vulnerabilities and their effects on a system. These concepts encourage the definition of criteria that allow comparison and evaluation of vulnerabilities-based security framework.

A Qualitative Analysis of an Ontology Based Issue Resolution System for Cyber Attack Management [51]

Authors presented ontology-based Issue Resolution System (IRS), which classifies information about attack vectors in order to facilitate communication within the organization. The IRS uses extended taxonomy of cyber-attacks, as a solution that addresses deficiencies in existing taxonomies. The goal of IRS is to provide the defender with attack vector details which include information regarding what comprises the attack and what impact an attack can have on target system. Information structure about attack vectors in form of a tree is formalized by information extraction and data mining techniques to display the entire attack path within the IRS. Authors have made validation of their IRS ontology using qualitative research of security experts.

A Security Audit Framework to Manage Information System Security [42]

In this article, the conceptual security framework for management and audit of information systems security is proposed and discussed. The proposed framework should primarily help organizations to understand what they exactly need to protect assets and what their vulnerabilities are, allowing performing appropriate security management. Furthermore, it should provide good basis for security audit in order to create support for organization to assess effectiveness of adopted policies and controls in order to prevent or mitigate attacks, threats and vulnerabilities resulted from progress of new technologies and new Internet-enabled services, which organization is subject to. The presented framework is based on conceptual model approach, which contains a semantic description of concepts defined in information security domain, based on ISO/IEC_JCT1 standard.

A Security Framework for Audit and Manage Information System Security [44]

This article discusses conceptual security framework for management and audit of information systems security. The proposed framework is based on conceptual model, according to ISO/IEC_JCT1 standard, in order to help organizations to manage better security of their information systems. The article presents an approach for improving security management by conceptual framework, developed to assist organizations to classify attacks, identify assets and mitigate their vulnerabilities and threats. Proposed framework is based on a conceptual model with the representation possibility of semantic concepts and their relations in the information security field, as defined in accordance with the established security standard ISO/IEC_JTCI1.

The proposed framework is based on conceptual ontology, which models basic concepts of attacks, threats and vulnerabilities, and their relationships with other security concepts. Defined conceptual model contains 8 concepts and 16 relations, based on the security standard ISO/IEC_JCT1.

A Security Ontology for Incident Analysis [6]

Authors have developed a security incidents ontology that takes into account the organization and its overall systems, not just software. This includes appropriate defensive classes with offensive categories of incidents since adverse outcomes also need to be considered from the standpoint of defenders, taking into account their objectives and specific circumstances. Three-level security architecture has been made, consisting of social, logical and physical level that allow planning of comprehensive defense measures with total area attacks that span across all levels. These ideas provide a holistic analysis of incidents, not only from technical aspects but including human and natural factors that can give a comprehensive defense-in-depth for prevention, detection, and recovery from incidents.

A Security Ontology with MDA for Software Development [29]

It has been noticed that an approach that includes security issues and concepts throughout development process is lacking, and, to overcome this deficiency, a security ontology for software development has been defined using Model Driven Architecture (MDA). This ontology was used in software development in such a way that security issues and concepts could play a role in each of the stages in the development process and that they could be included in software as security components. In this paper, authors first introduce the new ontology and its semantics, and then show how to use it in the development process using the example of four case studies. The results of case studies have shown that proposed security ontology can be used in modeling and designing security issues and concepts in each phase of the development process with MDA.

A Semantic-based Intrusion Detection Framework for Wireless Sensor Network [29]

In this study, a new intrusion detection framework for Wireless Sensor Network (WSN) has been introduced. The authors have tried to solve the problem of WSN's from a new perspective using multi-agent and semantic techniques. They proposed a layered architecture for a framework for detecting WSN attacks. Key framework components have been explained and security ontology, according to WSN features, was built, which represents a formal

semantics and is used to improve the process of detection of attacks for WSN. Also, several algorithms for intrusion detection were proposed, based on the structure of WSN, which solve the problem of detecting attacks through decentralized and cooperative mechanism.

A Study on Security and Ontology in Cloud Computing [28]

This paper discusses a detailed study about security measures and ways to improve security levels in both private and public clouds. Details of some security methods for data security in the cloud are described, and some methods to provide higher levels of security are proposed as well.

A user-oriented ontology-based approach for network intrusion detection [24]

In this paper, the authors propose a new approach for application design and development to detect attacks, which uses domain expertise for easier generation of intrusion detection. This approach allows the user to shape intrusion detection application on a conceptual level and in terms of concepts from the application domain. This is accomplished by using a domain ontology which captures domain knowledge. Domain ontology can be constructed by domain experts or through existing ontology. By using knowledge from domain ontology and set of high-level modeling concepts for intrusion detection modeling, a non-expert in the field of intrusion detection can specify intrusion detection system by placing instances of concepts in the domain ontology.

This approach has following advantages. First, it meets the demands of end users and customers better; second, the development process can be shortened; third, rapid prototyping is possible; fourth, better communication between intrusion detection experts is achieved; and finally, one can use knowledge from the domain. In addition, use of ontologies allows the incorporation of some intelligence and, therefore, intelligent reasoning about intrusion detection becomes possible.

An Efficient Network Security System through an Ontology Approach [2]

This paper describes the role of ontologies in facilitating network security modeling. It outlines the technical challenges in simulation modeling of distributed network security and describes how ontology-based methods can be applied to these challenges. The paper concludes with a description of the ontology-based framework for simulation modelling and analysis of network security and also states the advantages of this approach.

An Extended Ontology for Security Requirements [35]

The main objective of this paper is to join and expand two previously proposed security ontologies. Joining involves careful comparison of simple concepts, but also offers a new view of rather ambiguous security concepts, such as vulnerabilities and threats. New concepts are justified by reviewing relevant literature and proposed expanded ontology gathers those concepts to facilitate security argumentation that was not possible in each method due to non-existing constructs. Furthermore, the paper offers a series of security requirements adopted from industrial case studies, along with their associated representations in terms of proposed ontology.

An Information Security Ontology Incorporating Human-Behavioral Implications [41]

In this paper, the authors examine the need to understand factors of human behavior within the process of information security management in an organization. They developed an information security ontology that combined the content of external information security standards (in this case ISO 27002) with the explicit review of potential human-oriented security issues. This ontology provides a framework within which it is possible to explore behavioral implications of management decisions related to information security before setting up security controls. It can be concluded that in organizations the consolidation of information security policy with behavioral considerations is possible and that this process can be facilitated using the specialized ontology. The proposed ontology showed that expert

knowledge of usability factors in information security can be associated with properties of information security infrastructure.

An Ontological Approach Applied to Information Security and Trust [59]

The authors in this paper, by using an ontological approach, defined security ontologies as a common vocabulary that is meaningful to people and software agents. Furthermore, they presented basic security concepts and implications of trust and explained their security ontologies defined in OWL ontology language. The ontologies above include security asset-vulnerability ontology (SAVO), security algorithm-standard ontology (SASO), security function ontology (SFO) and security attack and defense ontologies (SAO and SDO).

The main ontology of these authors is the security asset-vulnerability ontology (SAVO), which shows how attacks on individual nodes may affect their assets protected by defense mechanisms, how threatening agents exploit vulnerabilities in order to execute attacks and how an asset is estimated using quantitative and qualitative analysis. SAVO, as the main security ontology, connects other security concepts, mechanisms and ontologies, including security attack ontology, security defense ontology, security algorithm-standard ontology, and security function ontology.

An Ontological Approach to Information Security Education [23]

This paper reports on the practice of teaching and training information security for students of software engineering and employees from the software industry. It proposes an ontological approach for teaching and training of software engineering students in information security and describes the advantages of knowledge organization and transformation it provides.

An Ontology-Based Approach to Information Security [43]

The paper aims to present a conceptual model of ontology implementation defined in the security domain. The presented model contains semantic concepts based on the information security standard ISO/IEC_JTC1, and their relationships with other concepts, defined in information security sub-domains. Adoption of ontological approach as the theoretical foundation and methodological tool represents promising new solutions in the information security field and should be discussed by the scientific community.

An Ontology-Based Approach to Information Systems Security Management [56]

In this paper, the authors laid the foundations for establishing a knowledge-based framework with ontology in its center, with respect to security management of the observed information system. The proposed framework includes information system security management by connecting high-level policy statement and low-level explicit security controls, adaptable and applicable in the information systems environment. In addition, the paper proposes an architecture that will facilitate the framework's implementation. The overall approach is laid out as following: 1. identify and define necessary framework's components and mechanisms; 2. collect security requirements resulting from policy statements and express them in a way rich with valuable information; 3. link security requirements with appropriate actions for risk reduction (i.e. some countermeasures); 4. enable implementation mechanisms of information system's infrastructure; 5. define architecture for information system security management.

This framework can support critical security professionals' activities, related to security requirements identification and selection of individual controls that relate to the particular information system. Also, there is a brief description of necessary steps to establish a proposed framework for information systems security management. It can be identified by four main stages of the process, namely: a) security ontology construction, b) security requirements collecting, c) security actions definition and d) security actions implementation and monitoring.

An Ontology-based Approach to the Formalization of Information Security Policies [12]

In this study the authors presented a structure of information security ontology and discussed the paradigm in which it can be used to extract knowledge from natural language texts, such as information security standards, security policies, and security control descriptions. In addition to providing a vocabulary for information security domain, the proposed ontology stores logical forms corresponding to statements in a text, as well as a set of axioms used for conclusion in descriptive logic. The descriptive logic is a term that refers to any of several logic languages that are usually used to represent knowledge. Authors also described a tool for providing automated support for formalization process.

Authors point out that this ontology is more than just a set of concepts constituting a vocabulary on the topic of information security. Its purpose is threefold: first, taxonomy storage for information security domain; second, storage of logical forms that represent actions in organization's security policy; and third, axioms storage to support the conclusions of descriptive logic. These elements (taxonomy, logical forms and axioms) are ultimately stored in an ontology in the form of concepts, properties and restrictions of descriptive logic.

An Ontology of Information Security [22]

In this article, authors present ontology that (1) provides a general overview of information security domain, (2) contains a detailed domain vocabulary that makes it possible to respond to queries on specific technical security issues and solutions, and (3) supports machine reasoning. Authors described OWL-based ontology using fundamental concepts of asset, threat, vulnerability, countermeasure, security objective and defense strategy and the ontology includes 88 classes of threats, 79 asset classes, 133 classes of countermeasures and 34 relations between these classes.

An Ontology for Network Security Attacks [50]

This article presents a framework for network security based on proven concepts. Based on the research made on network security services, threats, vulnerabilities and ways of failure, it is an extensive network security attacks ontology that shows the relationship among many standard classifications used.

An ontology for secure e-government applications [30]

This paper addresses issue of security requirements placement in application development and the authors propose the use of ontologies for recording and display of security experts' knowledge. In this way, developers can use security expertise for design choices preparation that will help them meet security requirements more effectively. In their work, authors point out that they have developed security ontologies for two different scenarios of application to illustrate its use.

An Ontology Framework for Managing Security Attacks and Defences in Component-Based Software Systems [61]

The authors have developed security ontologies specifying information on security issues, especially including security attacks and defense. The main security ontology called Security-Asset Vulnerability Ontology (SAVO) shows how intruders exploit vulnerabilities to carry out attacks against other network nodes or system. SAVO links high-level security policies with other security concepts, mechanisms and ontologies, including Security Attack Ontology (SAO), Security Defense Ontology (SDO), Security Algorithm-Standard Ontology (SASO) and Security Function Ontology (SFO) to define information security issues and help developers to create better and more efficient systems for protection against attacks and failures.

An Ontology-Driven Approach Applied to Information Security [60]

To achieve collaborative intrusion detection and defense in distributed environments, the system and its components should have a common mechanism for the exchange of gathered data about security attacks and countermeasures. Accordingly, the authors have developed

and applied security ontology that will serve as a common vocabulary for sharing and analyzing received information that is understandable to people and software agents. In particular, different security terms, concepts and mechanisms have been introduced through certain security ontologies, including Security-Asset Vulnerability Ontology (SAVO), Security Algorithm-Standard Ontology (SASO), Security Function Ontology (SFO), Security Attack Ontology (SAO) and Security Defense Ontology (SDO).

An OWL-based Security Incident Ontology [34]

In order to facilitate and even allow correlation of various security incidents from various sources, but also to facilitate knowledge and information management about security incidents, the authors proposed security incidents ontology by defining a unique vocabulary of concepts and relationships associated with this domain. Their security incidents ontology has been developed using Protégé 3.0 and OWL plugin available for this tool. The main classes of proposed security incidents ontology are: *access* (class represents type of access that agent may have), *agent* (an entity that performs one or more attacks in order to cause security incident), *asset* (this class is the objective of security incident), *attack* (this class represents an attack performed by an agent), *consequence* (possible consequences implied by security incident), *security incident* (the most important class that represents a security breach caused by attack agent), *time* (information on when security incident took place), *tool* (tool used by an agent for the exploitation of a computer system) and *vulnerability* (a class that represents types of vulnerabilities that a system may have).

Application of Security Ontology to Context-Aware Alert Analysis [67]

This paper deals with the analysis of alerts, which feature context awareness as one of their key functionalities. Today, we still lack a practical and effective approach that guarantees a unified view of the context, background and knowledge of attacks for the requirements of security alerts. The authors argue that their proposed approach improves existing alert analysis techniques by providing formal representation using security ontology, which could be an important phase in implementation of unified network security management.

Constructing Enterprise Information Network Security [32]

In this article the authors describe ontology for an information security risk management structure which is composed of three parts: domain ontology, tasks ontology and solutions ontology. This structure was established using the Protégé 3.1, and its purpose is to adopt such principles that expert knowledge in detecting attacks, network security techniques, security policies, etc., can be modelled, stored and shared, as well as available for queries. One of the goals of this paper is to provide subjective domain knowledge to decision makers for making optimal decisions related to security issues.

Data Center Physical Security Ontology for Automated Evaluation [27]

This article presents an ontology developed for knowledge sharing about information security, focusing on physical security of data center by collecting and mapping requests from known information security standards, such as COBIT, ISO/IEC 27002 and ITIL. Data center physical security ontology can be used for automated evaluation in the future to improve the automated process of harmonization, and also provides connection points for information security domain. Since information systems can be accessed by physical or logical way, information security should be divided into physical and logical security, by which, data center physical security is linked to the main information security domain in the area of physical security. In addition to the data center, there are other physical entities, such as customers, telecom assets, etc. Controls of these entities may also be developed as ontologies and link to information security domain in the physical security area.

Developing an Ontology of the Cyber Security Domain [40]

This paper reports on the authors' research of developing cyber security ontology from the initial malicious software ontology. They have first described cyber security ontology efforts and objectives, followed by a discussion on used ontology development methodology. Current cyber security ontology is primarily focused on malware and some preliminary aspects of so-called 'diamond model', which includes actors, victims, infrastructure and capabilities.

Formalizing Information Security Knowledge [17]

This article describes security ontology that provides the ontological structure of information security domain knowledge. Based on analyzed risk management approaches, existing literature and specific requirements for risk management, this ontology includes concepts of threats, vulnerabilities and controls, representing domain knowledge of information security. In addition to these basic concepts, it also includes concepts and relationships required to describe formally an organization and its assets.

In order to enrich a knowledge model with specific knowledge about information security, the authors have analyzed several best practice guidelines and information security standards in terms of their acceptance, integrity, availability and knowledge representation. Finally, the German IT Grundschutz standard has been selected and overlapped with security ontology by which more than 500 information security concepts and 600 corresponding formal axioms were integrated into the ontological knowledge base. The main challenge in knowledge integration has been related to differences of both knowledge models and inconsistent granularity of the German IT Grundschutz standards. The goal of developed security ontology is to provide a knowledge model, and therefore the knowledge base in information security domain, which includes the most relevant information security concepts (threats, vulnerabilities, assets, controls and their implementation).

Ontological Approach toward Cybersecurity in Cloud Computing [55]

In order to preserve cyber security in cloud computing, you need to identify and discuss cyber security of information to be exchanged in a cloud. For this purpose the authors propose an ontological approach to cyber security cloud computing. The proposed cyber security ontology for operational information is based on real cyber operations mainly focused on non-cloud computing. In order to discuss cyber security required in cloud computing, an ontology has been applied on cloud computing. Through discussion, authors found and identified three main factors that affect the cyber security in cloud computing, namely: data assets separation, multiple resources composition and use of external resources. Based on changes in cloud computing, the authors have identified information about cyber security that is necessary because of important changes, such as data origin and information about resource dependencies.

Ontological Mapping of Information Security Best-Practice Guidelines [18]

In this paper, the authors proposed a method for mapping guidelines of best practice and existing security ontologies. The method is demonstrated on mapping EBIOS and IT Grundschutz standards with security ontology: entities and their attributes are defined in both knowledge bases and assigned to appropriate concepts and relationships defined in security ontology. Using this mapping scheme, knowledge derived from EBIOS and IT Grundschutz standards can be transformed into OWL code used by security ontology. The proposed method for mapping information security knowledge is a guideline that tries to enrich existing security ontologies with widely accepted knowledge about information security. The limitations of this method are: (i) in case of unstructured knowledge sources (e.g. IT Grundschutz), it requires a lot of manual intervention and does not give a satisfactory degree of automation; (ii) attempt to incorporate more than one best practice guideline shows limitation of this methodology, i.e. even if one knowledge source can be semi-automatically incorporated, it requires a significant manual intervention in mapping further knowledge base on the existing body of knowledge.

Ontologies for information security management and governance [36]

The paper starts with a review of ways to influence security and security issue solving within an organization, as a complex and important task that most administrators cannot perform manually and it is necessary to provide some automatic way of normalization of concepts, relationships and attributes, which are used in information security field. Furthermore, based on decision-making structure in information systems, a three-tier framework is designed for building models of information security governance (ISG) where ontology can serve as basis for this. The authors describe ontology examples for all three management levels (strategic, tactical and operational) designed to represent knowledge at these levels. This includes vulnerability ontology (example for operational level), incident management ontology (example for tactical level) and security policy ontology (example for strategic level).

This paper shows that it is possible to use ontologies to represent information security concepts, and some of the prominent advantages of using ontologies in ISG, related to security administrator services are:

- Ontologies development creates a conceptual model that enables an organization to know better and understand its security domain.
- Ontologies can facilitate interoperability between different security tools, creating unique ways of presenting security data, which allows mapping of security data from any security tools into an ontology. The mapping process allows that any security tool can have its own security data structured in an ontology defined format.
- The security incidents ontology uses vulnerability ontology, demonstrating the capacity of knowledge and information re-use.
- Ontologies allow security administrators to learn from past security issues in a holistic manner, helping them in solving and preventing new issues.
- Continuous improvement of resolving process by the introduction of new rules about security incidents, vulnerabilities and policies will help security administrators in the development of the most appropriate solutions.

Finally, this paper suggests a possible framework in which stakeholders can participate in information security management on a more abstract level at which someone is not interested in security events per se but for the overall performance that may arise on organization's operations due to security events.

Ontologies for Modelling Enterprise Level Security Metrics [52]

The main objective of this research is to develop framework for security ontology to support analysis of IT security risk. Ontology should know which threats endanger which assets and which countermeasures can reduce the likelihood of attacks. In this ontology all assets and any countermeasures can be marked with different types of costs and benefits, and the ontology can provide a quantitative risk analysis so that the manager can choose appropriate safeguards to mitigate threats for the organization.

Ontology Based Approach for Perception of Network Security State [5]

This article presents an ontological approach for the perception of current network security state. The computer network is a dynamic entity whose status changes with the introduction of new services, installation of new network operating system and adding new hardware components, the creation of new user roles and attacks by various actors. Various security mechanisms used in networks do not give a complete picture of entire network's security. Authors have proposed a taxonomy and ontology that can be used for reasoning on the impact of various events in the network on the state of network security. Major taxonomic classes in ontology are a vulnerability, network, and attack. The proposed ontological approach is a simple and vulnerability-oriented approach that can be extended by taking into account the access control based on roles and defined malicious and normal state parameters.

Ontology based IT-security planning [19]

The authors presented a security ontology that allows SMEs to implement holistic IT security approach and noted two potential application areas of such an ontology. First, it can be used to define precise IT security terminology. Second, the ontology provides a framework for machine-readable knowledge storage about security domain and relevant infrastructure elements. Security ontology consists of five sub-ontologies: (1) attribute, (2) threat, (3) infrastructure, (4) role, and (5) person. Holistic security ontology can help to clarify meaning and interdependence of terms related to IT security and can integrate interdependence of threats, countermeasures and resources. The integration of these interdependencies is needed for modeling events that threaten existing resources.

Ontology Development for Business Impact Analysis in Information Technology Business Continuity Management for Public Sector in Malaysia [49]

This article describes a study in progress that refers to the development of ontologies for business impact analysis (BIA) in the field of business continuity management of information technology in the public sector in Malaysia.

Traditional BIA approach uses simple representations of information with check-lists, tables, questionnaires and survey forms. A more complex approach involves representation matrix, remodelling and business processes simulation and analytical methods. This research explores the approach of using ontologies in providing semantically rich knowledge representation for BIA. The result of this approach is establishing a common BIA vocabulary that would help business impact analysts. This study used a qualitative method for extracting and generating ontologies needed for BIA. Domain ontology is derived from related security ontologies and further adapted to the general business continuity management framework. The outcome of this research has been checked on the basis of qualitative data collected from stakeholders and domain experts such as risk analysts and business analysts involved in BIA process.

Ontology for attack detection: An intelligent approach to web application security [48]

The proposed attacks ontology and communication protocol ontology provide a powerful construct to improve detection capabilities of application level attacks. The proposed mechanism is a new approach that uses semantics in application layer security as opposed to traditional signature-based approach and has the following key contributions:

• Ontological model of communication protocol: ontological model of HTTP protocol takes specification context and is designed in such a way that it not only detects attacks of HTTP protocol specifications, but also helps the system to focus only on specific parts of HTTP requests and responses where the existence of a malicious code script is possible.

• Ontological model of attack: the model encompasses the context of important attacks on web applications, different technologies used by hackers, sources and targets, impact on system components affected by the attack, attack exploited vulnerabilities and controls in terms of mitigation policies of such attacks.

To assess the quality of proposed ontological models and to evaluate ontology, a comprehensive set of metrics is used.

Ontology for Detection of Web Attacks [31]

The authors of this paper were concerned with problems of existing Intrusion Detection System (IDS) i.e. low rate of false-positive alerts, low rate of false negative alerts and information overload, and discuss the use of semantic web in IDSs. A brief overview of various security techniques is presented, and established that the base of threat identification and recognition with great accuracy and the active response is of great significance in a security system. The authors found out that IDS systems are not adequate for the effective protection of intruders and that a semantic based IDS system is required, capable of making intelligent detection decisions based on target domain context. This study has aimed to take steps in the use of ontologies to identify Web attacks since authors argue that an ontological

system could be an effective solution for building integrated systems in an industrial world by combining firewall and IDS features.

Ontology-Based Model of Network and Computer Attacks for Security Assessment [20]

This paper provides an ontology-based model of attacks and uses it to evaluate information systems security from attacker's perspective. The authors have categorized attacks into a taxonomy suitable for security assessment. The proposed taxonomy consists of five dimensions, which include attack impact, attack vector, the target of attacks, vulnerability and defense. The next step was ontology building according to taxonomy, where attack concepts involved in five dimensions, as well as the relationships between them, were formalized and analyzed in detail. Also, the proposed attack ontology was populated with information from national vulnerability database (NVD) about vulnerabilities such as: common vulnerability enumeration (CVE), common weakness enumeration (CWE), common vulnerability scoring system (CVSS), and common platform enumeration (CPE). At the end of the paper an ontology-based framework is proposed for assessing security of network and computer systems and describing the use of ontologies in security assessment as well as the method of evaluating the effects of attack, when a system is attacked.

Ontology top-level concepts include vulnerability, IT product, attacker, attack, consequence and countermeasure. Specifically, vulnerability that exists in IT product can be used by an attacker, and attacker runs the attack with the aim of compromising IT products and, by doing that, causes security repercussions. Countermeasures can be used for the protection of IT products through mitigation of vulnerabilities.

Ontology-Based Security Standards Mapping Optimization by the Means of Graph Theory [45]

In this paper, the authors analyze existing solutions for harmonization of standards and security ontology in order to design adaptive mapping of security standards by using ontology and graph theory to visualize mapped standards. The architecture of a prototype was presented that was used to map ISO 27001 standard and the best core security practice. An experiment showed that the proposed model can reduce the need for standard documents mapping. The proposed solution can be useful for the further detailing of certain security standards control mechanisms in a wider area which, however, still depends on the security standards description in the basic ontology.

OVM: An Ontology for Vulnerability Management [64]

The proposed ontology for vulnerability management (OVM) is populated with all the vulnerabilities within the American National Vulnerability Database (NVD) with additional reasoning rules, knowledge representations and data mining mechanisms. Vulnerability ontology captures important concepts and relationships to describe vulnerabilities in the context of software and systems security. Top-level ontology concepts are: vulnerability, IT product, attacker, attack, consequence and countermeasure.

Security Attack Ontology for Web Services [62]

This paper describes security threats to Web services and states that they must be systematically analyzed and classified in order to enable development of better-distributed defense mechanisms for Web services using firewalls and intrusion detection systems (F/IDS). Authors have chosen ontology and OWL/OWL-S instead of taxonomy because ontologies enable the development of different sides and shared understanding of information that can be automatically reasoned and analyzed. Using the examples, the authors have illustrated the benefits of using developed security attack ontology for Web services.

Security Data Mining in an Ontology for Vulnerability Management [65]

The authors have developed an ontology for security vulnerabilities, which defines key concepts in managing vulnerabilities and their relationships. Within the ontology design and consideration has been introduced, with examples of vulnerability analysis and assessment.

The result of this study provides a promising way of making security automation using semantic technologies. The top-level ontology includes the following concepts: *vulnerability, IT product*, *attacker, attack, consequence* and *countermeasure*. More specifically, a *vulnerability* that exists in an *IT product* can be used by *attacker* carrying out *attacks* with the aim to compromise the *IT product* and provoke *consequences*. *Countermeasures* can be used to protect IT product through mitigation of *vulnerabilities*.

Security Ontologies: Improving Quantitative Risk Analysis [14]

The authors proposed security ontology to provide a solid basis for applicable and holistic approach to IT security for SMEs, enabling cost-sensitive risk management and threats analysis. Using this ontology, each threat scenario can be simulated with different protection profiles to assess the efficiency and cost-benefit of individual protective measures. This security ontology framework consists of four parts. The first part is based on Landwehrer's taxonomy of security and reliability, the second part is a fundamental methodology of risk analysis, the third part describes concepts of IT infrastructure domain while the fourth part provides simulations by enabling enterprises to analyze various scenarios. Proposed ontological-based approach allows company modelling by combining knowledge of security and business domains. Ontology ensures common and precise terminology and, when using OWL for its display, it also ensures portability. Knowledge about threats and appropriate countermeasures is integrated into the ontological framework.

Security Ontology Construction and Integration [9]

The authors have shown that an ontology can be designed and created in a way that will make it suitable for interoperability and integration. The Paper presents the collected requirements which it is necessary to take into account when creating ontologies, as well as a method of creating ontologies and criteria for the selection of keywords. An ontology created in such way should provide means for interoperability with other systems.

Security Ontology for Adaptive Mapping of Security Standards [46]

The use of security ontology for mapping different standards can reduce the complexity of mapping, however, the choice of security ontology is of paramount importance, and there is no analysis of security ontology suitability for adaptive standards mapping. The aim of this paper is to analyze adequacy of existing security ontologies for the use of adaptive security standards mapping and to propose a new ontology, more appropriate for this purpose. In this paper the authors also analyzed existing security ontologies by comparing their general properties, OntoMetric factors and possibilities of covering various security standards. Since none of analyzed security ontologies could cover more than one third of security standards, the authors have proposed a new security ontology which increased the coverage of security standards in comparison with the existing ontologies and had better branching and depth properties for ontology visualization purpose. During this study four security standards (ISO 27001, PCI DSS, ISSA 5173 and NISTIR 7621) were mapped with this new security ontology, which allowed for the use of this ontology and mapped data for adaptive mapping of any set of security standards for optimizing use of multiple security standards in an organization.

The above mentioned security standards were mapped to a new ontology in order to assess its appropriateness for security standards mapping. Using the proposed ontology, which has five top-level classes (asset, countermeasure, organization, threat and vulnerability), as basis for flexible mapping, 80% of 27001 and 100% of PCI DSS, ISSA 5173 and NISTIR 7621 standards were mapped into ontology. 100% mapping of ISO 27001 standard was not achieved, because very specific requirements of security standards (such as security features of used operating systems, etc.) were not mapped to an abstract level in the proposed ontology. The proposed security ontology also has a more balanced tree structure which also increases visualization capabilities.

Security ontology proposal for mobile applications [3]

In this paper, the authors first showed the results of research about vulnerabilities and attacks on mobile applications. Through a bottom-up methodology they have conducted a study about mobile applications security that brought them to a conceptualization based on ontology. Mobile security ontology is designed in accordance with three sub-ontological compositions that allow for reuse and sharing of additional fields of mobility. Through developed ontology they conceptualized not only semantic relations between actors and security services or goals they offer but also side effects of security on additional non-functional requirements.

The Design, Instantiation, and Usage of Information Security Measuring Ontology [16]

In this article, the authors present Information Security Measuring Ontology (ISMO), developed specifically for the purpose of measuring security runtime. The main objective was to achieve an ontology able to support measurement of security during application execution. The ontology development uses two existing ontologies: (i) information security ontology, which describes security-related concepts, and (ii) software measurement ontology, which describes general measurements terminology.

The STAC (Security Toolbox: Attacks & Countermeasures) Ontology [21]

The authors of this paper presented security ontology which should help non-security professionals who deal with software design or programming to: (1) design secure software, and (2) understand and be aware of main security concepts and issues. This security ontology defines main security concepts such as attacks, countermeasures, security features and their relationships. Countermeasures can be cryptographic concepts (e.g. encryption algorithms, key management, digital signature, hash function), security tools or security protocols. The purpose of this ontology is its reusability in a number of areas, such as Web application security, network management or communication networks (sensors, mobile and wireless networks). In short, this ontology defines relationships between the following concepts: application, request, domain, attack, countermeasure, property, security feature and OSI model.

Toward a Unified Ontology of Cloud Computing [68]

This paper discusses the area of cloud computing area, and proposes a detailed cloud computing ontology as an attempt to create domain knowledge in the field of cloud computing and its relevant components. Composability was used as a methodology for ontology building, which allowed authors to record the interconnections between various cloud components. The proposed ontology is represented by a number of cloud layers (applications, software environments, software infrastructure, software core (kernel) and hardware) and advantages, limitations and dependencies of each layer on previous computer concepts were discussed.

Towards an Ontology for Cloud Security Obligations [4]

This paper presents an ontology for cloud security obligations, based on a range of industry accepted standards and guidelines, and includes security controls that can be offered by providers of public services in a cloud. The aim of this paper was to review this ontology, as well as highlight some of its possible applications. The established ontology for cloud security obligations has a broad scope and will help to clarify specific security obligations, and can also be used as a basis for risk analysis for procurement teams in a cloud. In addition, clarifying and formalizing security obligations for service providers in the cloud will also allow for comparison of different service offerings in a cloud in an automated way. In longer term, the authors predict that adoption of common ontology security requirements in a cloud among providers will open possibilities for independent providers in a cloud to identify, integrate and customize cloud services according to the clients' needs.

The limitation of the current version of this ontology is its current focus on security obligations for service providers in a cloud. However, a service provider may also require

their clients to follow certain obligations ("Terms of Use"), which could also be integrated with the ontology. It should also be kept in mind that obligations in this ontology are only technical security controls that can be implemented in a cloud, and do not include all issues related to, e.g. policies and procedures, risk assessment or corporate security management. In addition, authors' focus was only on security and ontology does not include any obligations concerning e.g. reliability and performance of services in a cloud.

Towards an Ontology-based Security Management [57]

This article describes a framework for acquisition and management of security knowledge. It defines a kind of knowledge container, based on standards (security ontology) that extend the existing model with ontological semantics and can be used for reusable interoperability, aggregation and security knowledge reasoning, using security knowledge from different sources. In addition, separation of security requirements for technical implementation facilitates security management, and the authors provide a viable framework that connects high-level policies and security controls deployed as needed and facilitates security experts' work. The authors have fully implemented security ontology relating to vulnerability assessment and have shown that data extraction about security from high-level policies is viable.

3. Discussion and Conclusion

Security of information systems has gradually become a very wide research field and a discipline that allows building of reliable systems that can deal with malicious activity or errors. Information systems security domain also includes a variety of methods, techniques and tools responsible for the protection of information systems resources by ensuring availability, confidentiality, integrity and traceability of information. With a growing need for implementation of IT security measures in business environments around the world and with an increasing range of applications, the main obstacles faced by average analysts and programmers who use existing frameworks for modelling and analysis of security requirements, is a lack of security knowledge and expertise [53]. The cumulative knowledge of the information security community about the classification of threats, their prevention and defense against computer attacks should be formalized and stored in an appropriate form, reusable and applied in required time [47].

Ensuring information security and privacy ceased to be a subject of a narrow area of interest of information systems designers and become one of the key issues fundamental to the modern society. These security requirements must be carefully considered, not as isolated aspects, but as elements that must be present at all stages of a development lifecycle, from requirements analysis to implementation and maintenance. Application of ontological engineering in information security domain provides better knowledge organization and mechanisms for predicting security issues [7].

Development and application of ontology promotes the creation of a uniform standard for presentation of concepts within a particular knowledge domain. Within information systems security, use of ontology for formalization and presentation of information security concepts is a challenge for mechanisms and techniques that are currently used. The ontologically based approach introduces new perspective for data modeling in the security domain and provides a description of data semantics in a machine-accessible way. In information security context, ontology application contributes to the uniformity of terminology included in classification and security data store [43].

There are three main advantages of using ontologies. First, ontology organizes and systematizes all phenomena within the research scope (such as types of attack) at any level of detail, and reduces a huge variety of concepts to a much smaller list of properties. Second, most of approaches derived from induced modularity, for example by linking certain measures for detection of certain properties (e.g. if some attack properties require certain measures, complex attacks with set of properties, will require a matching set of countermeasures). Third, by providing full combinations of compatible properties, the

ontologically based approach can predict their amendments (for example, possible types of attacks that have not yet occurred) [47]. Additional reasons that support proposal of ontological approach within an information security management scope are the following [43], [61]:

- Ontologies allow determination of semantic relations between different concepts;
- Ontologies share common understanding of structured information between different parties, such as people or software agents, which allows automatic reasoning and analysis;
- Ontologies are reusable and can be improved over time;
- Ontologies are shared among different agents to solve interoperability problems.

As demonstrated by this research, there are many papers whose authors have dealt with the issue of formalization of a complete information security domain or one of its parts. This paper provides a literature review of this research area and identifies a total of 52 papers systematized in three groups: general security ontologies (12 papers), specific security ontologies (32 papers) and theoretical works (8 papers). The articles were of different quality and detail level and varied from simple conceptual ideas to sophisticated ontology-based frameworks. Also, within the papers there are some that are very similar, and these were written by the authors which first published them in scientific conference proceedings, and then, in a somewhat modified form, in scientific journals (e.g. [8], [7]), or are a simple upgrade of previous papers by the same authors (e.g. [42], [44], [59], [60]). A list of papers analyzed in this article, along with a brief overview of each paper, is presented in Table 2.

No.	Analyzed papers	Overview
1.	A Bootstrapping Approach for Developing a Cyber-Security Ontology Using Textbook Index Terms	The authors presented a bootstrapping method for development of cyber security ontology using a security textbooks index that gives a list of terms in the security domain and existing security ontology as a foundation.
2.	A Modeling Ontology for Integrating Vulnerabilities into Security Requirements Conceptual Foundations	The article proposes a modeling ontology focused on vulnerabilities, which aims to integrate empirical knowledge about vulnerabilities in the system development process.
3.	A Qualitative Analysis of An Ontology Based Issue Resolution System for Cyber Attack Management	The authors presented ontology-based Issue Resolution System (IRS), which classifies information about attack vectors and whose goal is to provide the defender with attack vector details regarding what comprises the attack and what impact an attack can have on the target system.
4.	A Security Audit Framework to Manage Information System Security	The authors propose and discuss a conceptual security framework for management and audit of information systems security, which contains a semantic description of concepts defined in information security domain, based on ISO/IEC_JCT1 standard.
5.	A Security Framework for Audit and Manage Information System Security	The article presents a framework for improving security management based on conceptual ontology, which models basic concepts of attacks, threats and vulnerabilities and their relationships with other security concepts. Defined conceptual model contains 8 concepts and 16 relations, based on the security standard ISO/IEC_JCT1.
6.	A Security Ontology for Incident Analysis	The authors have developed a security incidents ontology that takes into account the organization and its systems fully (not just its software). Three-level security architecture has been made, consisting of social, logical and physical levels that allow planning of comprehensive defense measures with total area attacks that span across all levels.
7.	A Security Ontology with MDA for Software Development	The authors define a security ontology for software development with Model Driven Architecture (MDA) that was used in software development so that security issues and concepts could play a role in each of stage in the development process and can be included as a security component in software.
8.	A Semantic-based Intrusion Detection	In this paper, a new intrusion detection framework for Wireless

No.	Analyzed papers	Overview
	Framework for Wireless Sensor Network	Sensor Network (WSN) has been introduced, using multi-agent and semantic techniques. Key framework components have been explained and a security ontology, according to WSN features, is built, which represents a formal semantics and is used to improve the process of detection of attacks for WSN.
9.	A Study on Security and Ontology in Cloud Computing	This paper discusses a study about security measures and ways to improve security levels in a cloud. Details of some security methods for data security in a cloud are given, and some methods to provide higher levels of security are also proposed.
10.	A user-oriented ontology-based approach for network intrusion detection	The authors propose a new approach for application design and development to detect attacks, which uses domain expertise for easier generation, which allows user to shape intrusion detection application on a conceptual level and in terms of concepts from the application domain.
11.	An Efficient Network Security System through an Ontology Approach	The paper describes an ontology-based framework for simulation modelling and analysis of network security and states the advantages of this approach.
12.	An Extended Ontology for Security Requirements	The authors present an expanded ontology that joins and expands two previously proposed security ontologies.
13.	An Information Security Ontology Incorporating Human-Behavioral Implications	The authors develop an information security ontology that combines the content of external information security standards with an explicit review of potential human-oriented security issues.
14.	An Ontological Approach Applied to Information Security and Trust	The authors present basic security concepts and implications of trust and explain their security ontologies defined in OWL ontology language that includes the security asset-vulnerability ontology, security algorithm-standard ontology, security function ontology and security attack and defense ontologies.
15.	An Ontological Approach to Information Security Education	This paper proposes an ontological approach for teaching and training of software engineering students about information security to display the advantage of knowledge organization and transformation.
16.	An Ontology Based Approach to Information Security	This paper presents a conceptual model of ontology implementation defined in security domain which contains semantic concepts based on information security standard ISO/IEC_JTC1
17.	An Ontology-Based Approach to Information Systems Security Management	The authors laid foundations for establishing a knowledge-based framework with ontology in its center, with respect to security management of the observed information system. They showed that it was possible to connect high-level policy statements and low-level explicit security controls with achievable implementation. Also, there is a brief description of necessary steps to establish a proposed framework for information systems security management. Four main stages can be identified in the complete process, namely: a) security ontology construction, b) security requirements collecting, c) security actions definition and d) security actions implementation and monitoring.
18.	An Ontology-based Approach to the Formalization of Information Security Policies	In this study the authors present a structure of information security ontology and discuss the paradigm in which it can be used to extract knowledge from natural language texts, such as information security standards, security policies and security control descriptions. The purpose of this ontology is threefold: first, taxonomy storage for information security domain; second, storage of logical forms that represent actions in organization's security policy; and third, axiom storage to support conclusion of descriptive logic.
19.	An Ontology of Information Security	The authors present an ontology that (1) provides a general overview of information security domain, (2) contains a detailed domain vocabulary which makes it able to respond to queries on specific, technical security issues and solutions, and (3) supports machine reasoning. The ontology includes 88 classes of threats, 79 asset classes, 133 classes of countermeasures and 34 relations between these classes.
20.	An Ontology for Network Security	This article proposes an extensible network security attacks

No.	Analyzed papers	Overview
	Attacks	ontology that shows relationships among many standard classifications, based on the research made on network security services, threats, vulnerabilities and ways of failure.
21.	An ontology for secure e-government applications	The authors propose the use of ontology for recording and display of security experts' knowledge regarding the issue of security requirements placement in application development.
22.	An Ontology Framework for Managing Security Attacks and Defences in Component Based Software Systems	The authors have developed security ontologies specifying information on security issues, especially including security attacks and defense. The main security ontology called Security-Asset Vulnerability Ontology shows how intruders exploit vulnerabilities to carry out attacks against other network nodes or systems. It links high-level security policies with other security concepts, mechanisms and ontologies, including Security Attack Ontology, Security Defense Ontology, Security Algorithm-Standard Ontology and Security Function Ontology to define information security issues and help developers to create better and more efficient systems for protection against attacks and failures.
23.	An Ontology-Driven Approach Applied to Information Security	The authors have developed security ontologies that will serve as a common vocabulary for sharing and analyzing received information. Different security terms, concepts and mechanisms have been introduced through certain security ontologies, including Security-Asset Vulnerability Ontology, Security Algorithm-Standard Ontology, Security Function Ontology, Security Attack Ontology and Security Defense Ontology.
24.	An OWL-based Security Incident Ontology	The authors have proposed a security incidents ontology, by defining unique vocabulary of concepts and relationships associated with this domain in order to facilitate correlation of various security incidents from various sources and to facilitate knowledge and information management about security incidents.
25.	Application of Security Ontology to Context-Aware Alert Analysis	The authors have proposed an approach for improving existing alert analysis techniques by providing formal representation using security ontology.
26.	Constructing Enterprise Information Network Security	The article describes an ontology for an information security risk management structure which is composed of three parts: domain ontology, tasks ontology and solutions ontology.
27.	Data Center Physical Security Ontology for Automated Evaluation	This article presents an ontology developed for knowledge sharing about information security, focusing on physical security of data center by collecting and mapping requests from known information security standards, such as COBIT, ISO/IEC 27002 and ITIL.
28.	Developing an Ontology of the Cyber Security Domain	This paper reports on authors' research of developing cyber security ontology from initial malicious software ontology. Current cyber security ontology is primarily focused on malware and some preliminary aspects of so-called 'diamond model', which includes actors, victims infrastructure and capabilities.
29.	Formalizing Information Security Knowledge	This article describes a security ontology that provides ontological structure of information security domain knowledge. Based on analyzed risk management approaches, existing literature and specific requirements for risk management, this ontology includes concepts of threats, vulnerabilities and controls, representing domain knowledge of information security.
30.	Ontological Approach toward Cyber security in Cloud Computing	In this article, the authors propose an ontological approach to cyber security cloud computing. Through discussion, they found and identified three main factors that affect the cyber security in cloud computing, namely: data assets separation, multiple resources composition and use of external resources.
31.	Ontological Mapping of Information Security Best-Practice Guidelines	In this paper, the authors propose a method for mapping guidelines of best practice and existing security ontologies. The method is demonstrated on mapping EBIOS and IT Grundschutz standards with security ontology**:** entities and its

No.	Analyzed papers	Overview
		attributes defined in both knowledge bases are assigned to appropriate concepts and relationships defined in the security ontology. Using this mapping scheme, knowledge derived from EBIOS and IT Grundschutz standards can be transformed into OWL code used by a security ontology.
32.	Ontologies for information security management and governance	Based on decision-making structure in information systems, the authors have designed a three-tier framework for building models of information security governance where ontology can serve as a basis for this building. Also, the authors describe ontology examples for all three management levels (strategic, tactical and operational) designed to represent knowledge at these levels. These include vulnerability ontology (example for operational level), incident management ontology (example for tactical level) and security policy ontology (example for strategic level).
33.	Ontologies for Modeling Enterprise Level Security Metrics	This article proposes a framework for security ontology to support analysis of IT security risk. In this ontology all assets and any countermeasures can be marked with different types of costs and benefits, and the ontology can provide a quantitative risk analysis so that the manager can choose appropriate safeguards to mitigate threats for organization.
34.	Ontology Based Approach for Perception of Network Security State	This article presents an ontological approach for perception of current network security state in the form of taxonomy and ontology that can be used for reasoning on the impact of various events in network on the state of network security. Major taxonomic classes in ontology are vulnerability, network and attack.
35.	Ontology based IT-security planning	The authors have presented a security ontology that allows SMEs to implement holistic IT security approach and have noted two potential application areas of such an ontology. First, it can be used to define precise IT security terminology. Second, the ontology provides a framework for machine-readable knowledge storage about security domain and relevant infrastructure elements. Security ontology consists of five sub-ontologies: (1) attribute, (2) threat, (3) infrastructure, (4) role, and (5) person.
36.	Ontology Development for Business Impact Analysis in Information Technology Business Continuity Management for Public Sector in Malaysia	This research explores the approach of using ontologies in providing semantically rich knowledge representation for Business Impact Analysis (BIA) in the field of business continuity management. The result of this approach is the establishment of a common BIA vocabulary that would help business impact analysts.
37.	Ontology for attack detection: An intelligent approach to web application security	The proposed attacks ontology and communication protocol ontology provide a powerful construct to improve detection capabilities of application level attacks. The proposed mechanism is a new approach that uses semantics in application layer security as opposed to the traditional signature-based approach.
38.	Ontology for Detection of Web Attacks	This article identifies the need of taking certain steps in the use of ontologies to identify Web attacks as the authors argue that ontological system could be an effective solution for building integrated system in the industrial world by combining firewall and Intrusion Detection System (IDS) features.
39.	Ontology-Based Model of Network and Computer Attacks for Security Assessment	This paper provides an ontology-based model of attacks used to evaluate information systems security from the attack perspective. The authors have categorized attacks into a taxonomy suitable for security assessment after which an ontology was built according to this taxonomy. In the ontology the attack concepts involved in five dimensions as well as the relationships between them were formalized and analyzed in detail. Ontology top-level concepts include vulnerability, IT product, attacker, attack, consequence and countermeasure.
40.	Ontology-Based Security Standards Mapping Optimization by the Means of Graph Theory	In article an architecture of prototype that was used to map ISO 27001 standard and Grundschutz best practice was presented, based on analyzed existing solutions for harmonization of

No.	Analyzed papers	Overview
		standards and security ontology in order to design adaptive mapping of security standards by using ontology and graph theory to visualize mapped standards.
41.	OVM: An Ontology for Vulnerability Management	This article proposed an ontology for vulnerability management (OVM) which is populated with all the vulnerabilities within the American National Vulnerability Database with additional reasoning rules, knowledge representation and data mining mechanisms. Top-level ontology concepts are: vulnerability, IT product, attacker, attack, consequence and countermeasure.
42.	Security Attack Ontology for Web Services	This paper describes an ontology of security attacks on Web services based on described security threats to Web services that must be systematically analyzed and classified in order to enable development of better distributed defense mechanisms.
43.	Security Data Mining in an Ontology for Vulnerability Management	The authors developed an ontology for security vulnerabilities, which defines key concepts in managing vulnerabilities and their relationships. Top-level ontology includes the following concepts: *vulnerability, IT product*, *attacker, attack, consequence* and *countermeasure*. More specifically, a *vulnerability* that exists in the *IT product* can be used by *attacker* carrying out *attacks* with the aim to compromise the *IT product* and provoke *consequences*. *Countermeasures* can be used to protect an IT product through mitigation of *vulnerabilities*.
44.	Security Ontologies: Improving Quantitative Risk Analysis	The authors proposed a security ontology to provide a solid basis for applicable and holistic approach to IT security for SMEs, enabling cost-sensitive risk management and threats analysis.
45.	Security Ontology Construction and Integration	The authors have shown that the ontology can be designed and created in a way that will make it suitable for interoperability and integration. The paper presents the collected requirements necessary to take into account when creating ontologies, as well as a method of creating ontologies and criteria for the selection of keywords.
46.	Security Ontology for Adaptive Mapping of Security Standards	The authors have proposed a new security ontology for adaptive security standards mapping which increased the coverage of security standards in comparison with existing ontologies and had better branching and depth properties for ontology visualization purpose.
47.	Security ontology proposal for mobile applications	In this paper, authors showed results of research about vulnerabilities and attacks on mobile applications through a bottom-up methodology that brought them to conceptualization based on ontology. Mobile security ontology is designed in accordance with three sub-ontological compositions that allow reuse and sharing of additional fields of mobility.
48.	The Design, Instantiation, and Usage of Information Security Measuring Ontology	The authors present the Information Security Measuring Ontology (ISMO), developed specifically for the purpose of measuring security runtime. The ontology development uses two existing ontologies: (i) information security ontology, which describes security-related concepts, and (ii) software measurement ontology, which describes general measurements terminology.
49.	The STAC (Security Toolbox: Attacks & Countermeasures) Ontology	The authors of this paper presented a security ontology which should help non-security professionals who deal with software design or programming to: (1) design secure software, and (2) understand and be aware of main security concepts and issues. This security ontology defines main security concepts such as attacks, countermeasures, security features and their relationships.
50.	Toward a Unified Ontology of Cloud Computing	This paper proposes a detailed cloud computing ontology as an attempt to create domain knowledge in the field of cloud computing and its relevant components which is represented by a number of cloud layers (applications, software environments, software infrastructure, software core (kernel) and hardware).
51.	Towards an Ontology for Cloud Security Obligations	This paper presents an ontology for cloud security obligations, which is based on a range of industry accepted standards and

No.	Analyzed papers	Overview
		guidelines, and includes security controls that can be offered by providers of public services in a cloud.
52.	Towards an Ontology-based Security Management	This article describes a framework for the acquisition and management of security knowledge i.e. it defines a kind of a knowledge container based on standards (security ontology) that extend the existing model with ontological semantics.

Table 2. Summary of analyzed papers with a short overview. Source: authors' representation

A recognized limitation of this study is the fact that, during the analysis of the research problem, only articles published in the last 10 years and available to the authors through scientific journals database research were taken into consideration, which means that there is a possibility of existence of other relevant articles that, due to certain reasons, did not enter this analysis. These reasons may be: relevant articles were found, but they were not free; articles were not indexed in the observed scientific databases; title and keywords have not represented the article's topic. Despite the fact that improvement is always possible, this work represents a good basis for further detailed research of ontological concepts in information security. Results of some of the analyzed articles revealed the gap between the areas of security requirements engineering and ontologies, and thus a new field of research. In addition, a proposal for future work is to provide an extended classification of security ontologies that would, among other things, specify them in detailed subgroups of specific security ontologies.

References

[1] Aaltonen, J; Krone, O; Mustonen, P. Towards Information Security Ontology in Business Networks. In *Proceedings of the 2009 conference on Information Modelling and Knowledge Bases XX*, pages 366–372, 2009.

[2] Azni, A. H; Saudi, M. M; Azman, A; Tamil, E. M; Yamani, M; Idris, I. An Efficient Network Security System through an Ontology Approach. In *Proceedings of the 2008. International Conference on Innovations in Information Technology*, pages 267–271, Al Ain, United Arab Emirates, 2008.

[3] Beji, S; El Kadhi, N. Security Ontology Proposal for Mobile Applications. In *Tenth International Conference on Mobile Data Management: Systems, Services and Middleware*, pages 580–587, Taipei, Taiwan, 2009.

[4] Bernsmed, K; Undheim, A; Meland, P. H; Jaatun, M. G. Towards an Ontology for Cloud Security Obligations. In *2013 International Conference on Availability, Reliability and Security*, pages 577–581, Regensburg, Germany, 2013.

[5] Bhandari, P; Singh, M. Ontology Based Approach for Perception of Network Security State. In *2014 Recent Advances in Engineering and Computational Sciences (RAECS)*, vol. 6913, pages 1–6, Chandigarh, India, 2014.

[6] Blackwell, C. A security ontology for incident analysis. In *Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research - CSIIRW '10*, pages 46–49, Oak Ridge, Tennessee, 2010.

[7] 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. Interfaces*, 33(4): 372–388, 2011.

[8] Blanco, C; Lasheras, J; Valencia-Garc, R; Fern, E; Toval, A; Piattini, M. A Systematic Review and Comparison of Security Ontologies. In *2008 Third International Conference on Availability, Reliability and Security*, pages 813–820, Barcelona, Spain, 2008.

[9] Boinski, T; Orlowski, P; Szymanski, J; Krawczyk, H. Security Ontology Construction and Integration. In *Proceedings of the International Conference on Knowledge Engineering and Ontology Development (KEOD)*, pages 369–374, Paris, France, 2011.

[10] Breitman, K; Casanova, M. A; Truszkowski, W. *Semantic Web: Concepts, Technologies and Applications*. Springer-Verlag, London, 2007.

[11] Brotby, K. *Information Security Governance: A Practical Development and Implementation Approach*. Hoboken, New Jersey: John Wiley & Sons, Inc., 2009.

[12] do Amaral, F. N; Bazílio, C. An ontology-based approach to the formalization of information security policies. In *Proceedings of the 10th IEEE International Enterprise Distributed Object Computing Conference Workshops, EDOCW '06.*, pages 1-8, Hong Kong, China, 2006.

[13] Ehrig, M. *Ontology Alignment: Bridging the Semantic Gap Computing for Human Experience*. Springer Science+Business Media, 2007.

[14] Ekelhart, A; Fenz, S; Klemen, M; Weippl, E. Security Ontologies: Improving Quantitative Risk Analysis. In *2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07)*, pages 156–163, Waikoloa, Hawaii, 2007.

[15] Elahi, G; Yu, E; Zannone, N. A modeling ontology for integrating vulnerabilities into security requirements conceptual foundations. In *Proceedings of the 28th International Conference on Conceptual Modeling*, pages 99–114, Gramado, Brazil, 2009.

[16] Evesti, A; Ovaska, E. The design, instantiation, and usage of information security measuring ontology. In *Proceedings of the 4th IEEE International Conference on Self-Adaptive and Self-Organizing Systems (SASO)*, pages 204 – 212, Budapest, Hungary, 2010.

[17] Fenz, S; Ekelhart, A. Formalizing information security knowledge. In *Proceedings of the 4th International Symposium on Information, Computer, and Communications Security - ASIACCS '09*, pages 183–194, Sydney, Australia, 2009.

[18] Fenz, S; Pruckner, T; Manutscheri, A. Ontological mapping of information security best-practice guidelines. In *Proceedings of the 12th International Conference on Business Information Systems (BIS 2009)*, pages 49–60, Poznan, Poland, 2009.

[19] Fenz, S; Weippl, E. Ontology based IT-security planning. In *Proceedings of the 12th Pacific Rim International Symposium on Dependable Computing (PRDC'06)*, pages 389–390, Riverside, California, 2006.

[20] Gao, J; Zhang, B; Chen, X; Luo, Z. Ontology-based model of network and computer attacks for security assessment. *J. Shanghai Jiaotong Univ.* 18(5):554–562, 2013.

[21] Gyrard, A; Bonnet, C; Boudaoud, K. The STAC (Security Toolbox: Attacks & Countermeasures) ontology. In *Proceedings of the 22nd international conference on World Wide Web companion*, pages 165–166, Rio de Janeiro, Brazil, 2013.

[22] Herzog, A; Shahmehri, N; Duma, C. An ontology of information security, *Int. J. Inf. Secur. Priv.* 1(4):1–23, 2007.

[23] Hu, H; Yang, M; Ge, Y; Xiang, H; Fu, L. An Ontological Approach to Information Security Education. In *Proceedings of the 2nd International Conference on Future Computers in Education*, pages 160–165, Shanghai, China, 2012.

[24] Hung, S.-S; Shing-Min Liu, D. A user-oriented ontology-based approach for network intrusion detection, *Comput. Stand. Interfaces*. 30(1–2):78–88, 2008.

[25] International Organization for Standardization. *ISO/IEC 27002: Information technology - Security techniques - Code of practice for information security management*, 2005.

[26] IT Governance Institute. *Information Security Governance: Guidance for Boards of Directors and Executive Managment, 2nd Edition*. ISACA, Rolling Meadows, Illinois, 2006.

[27] Janpitak, N; Sathitwiriyawong, C. Data Center Physical Security Ontology for Automated Evaluation. In *Proceedings of The 2011 International Conference on Security and Management (SAM'11)*, Las Vegas, Nevada, 2011.

[28] Kamalakannan, E; Prabhakaran, B; Arvind, K. A Study on Security and Ontology in Cloud Computing, *Int. J. Adv. Res. Comput. Commun. Eng.* 2(10): 3877–3882, 2013.

[29] Kang, W; Liang, Y. A Security Ontology with MDA for Software Development. In *Proceedings of the 2013 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery*, pages 67–74, Beijing, China, 2013.

[30] Karyda, M; Balopoulos, T; Dritsas, S; Gymnopoulos, L; Kokolakis, S; Lambrinoudakis, C; Gritzalis, S. An ontology for secure e-government applications. In *Proceedings of the First International Conference on Availability, Reliability and Security (ARES'06)*, pages 1033–1037, Vienna, Austria, 2006.

[31] Khairkar, A. D; Kshirsagar, D. D; Kumar, S. Ontology for Detection of Web Attacks. In *Proceedings of the 2013 International Conference on Communication Systems and Network Technologies*, pages 612–615, Thatipur, Gwalior, India 2013.

[32] Liu, F; Lee, W. Constructing Enterprise Information Network Security Risk Management Mechanism by Ontology. *Tamkang J. Sci. Eng.* 13(1):79–87, 2010.

[33] Mao, Y. A Semantic-based Intrusion Detection Framework for Wireless Sensor Network. In *Proceedings of the 2010 6th International Conference on Networked Computing (INC)*, pages 1–5, Gyeongju, Korea, 2010.

[34] Martimiano, L. A. F; Moreira, E. An OWL-based Security Incident Ontology. In *Proceedings of the Eighth International Protege Conference*, pages 1–4, Madrid, Spain, 2005.

[35] Massacci, F; Mylopoulos, J; Paci, F; Tun, T. T; Yu, Y. An Extended Ontology for Security Requirements. In *Proceedings of the CAiSE 2011 International Workshops*, pages 622–636, London, UK, 2011.

[36] Moreira, E. D. S; Martimiano, L. A. F; Brandão, A. J. D. S; Bernardes, M. C. Ontologies for information security management and governance, *Inf. Manag. Comput. Secur.* 16(2):150–165, 2008.

[37] Nascimento, C; Ferraz, F; Assad, R. OntoLog: Using Web Semantic and Ontology for Security Log Analysis. In *Proceedings of the Sixth International Conference on Software Engineering Advances, ICSEA 2011*, pages 177–182, Barcelona, Spain, 2011.

[38] Nguyen, V. Ontologies and Information Systems: A Literature Survey, DSTO–TN–1002, Defence Science and Technology Organisation, Edinburgh, South Australia, 2011.

[39] Noy, N; McGuinness, D. *Ontology development 101: A guide to creating your first ontology*, Stanford University, Stanford, California, 2001.

[40] Obrst, L; Chase, P; Markeloff, R. Developing an Ontology of the Cyber Security Domain. In *Workshop Proceedings of Semantic Technologies for Intelligence,*

Defense, and Security (STIDS), volume 966 of CEUR, pages 49–56, Fairfax, Virginia, 2012.

[41] Parkin, S. E; Van Moorsel, A. An Information Security Ontology Incorporating Human-Behavioral Implications. In *Proceedings of the 2nd international conference on Security of information and networks*, pages 46–55, Famagusta, Cyprus, 2009.

[42] Pereira, T; Santos, H. A Security Audit Framework to Manage. In *Proceedings of the 6th International Conference, ICGS3 2010*, pages 9–18, Braga, Portugal, 2010.

[43] Pereira, T; Santos, H. An Ontology Based Approach to Information Security. In *Proceedings of the Third International Conference, MTSR 2009,* pages 183–192, Milan, Italy, 2009.

[44] Pereira, T. S. M; Santos, H. A Security Framework for Audit and Manage Information System Security. In *2010 IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology*, pages 29–32, Toronto, Canada, 2010.

[45] Ramanauskaite, S; Goranin, N; Čenys, A; Olifer, D. Ontology-Based Security Standards Mapping Optimization by the Means of Graph Theory. In *Proceedings of the International Congress on Engineering and Technology*, pages 74–83, Dubrovnik, Croatia, 2013.

[46] Ramanauskaitė, S; Olifer, D; Goranin, N; Čenys, A. Security Ontology for Adaptive Mapping of Security Standards Security Ontology. *Int. J. Comput. Commun. Control*. 8(6):878–890, 2013.

[47] Raskin, V; Hempelmann, C. F; Triezenberg, K. E; Nirenburg, S. Ontology in information security: a useful theoretical foundation and methodological tool. In *Proceedings of the New Security Paradigms Workshop 2001*, pages 53–59, Cloudcroft, New Mexico, 2001.

[48] Razzaq, A; Anwar, Z; Ahmad, H. F; Latif, K; Munir, F. Ontology for attack detection: An intelligent approach to web application security. *Comput. Secur.* 45:124–146, 2014.

[49] Sabtu, S. B. M; Samy, G. N; Shanmugam, B. Ontology Development for Business Impact Analysis in Information Technology Business Continuity Management for Public Sector in Malaysia. In *Proceedings of the 13th International Conference on Applied Computer and Applied Computational Science (ACACOS '14)*, pages 215–220, Kuala Lumpur, Malaysia, 2014.

[50] Simmonds, A; Sandilands, P; van Ekert, L. An Ontology for Network Security Attacks. In *Proceedings of the Second Asian Applied Computing Conference*, pages 317–323, Kathmandu, Nepal, 2004.

[51] Simmons, C. B; Shiva, S. G; Simmons, L. L. A Qualitative Analysis of An Ontology Based Issue Resolution System for Cyber Attack Management. In *International Conference on Cyber Technology in Automation Control and Intelligent Systems (IEEE Cyber)*, Hong Kong, China, 2014.

[52] Singhal, A; Wijesekera, D. Ontologies for Modeling Enterprise Level Security Metrics Categories and Subject Descriptors. In *Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research*, pages 5–7, Oak Ridge, Tennessee, 2010.

[53] Souag, A; Salinesi, C; Comyn-Wattiau, I. Ontologies for Security Requirements: A Literature Survey and Classification. In *Proceedings of the CAiSE 2012 International Workshops*, pages 61–69, Gdansk, Poland, 2012.

[54] Stoll, M. Development of Stakeholder Oriented Corporate Information Security Objectives. In *Innovations and Advances in Computer, Information, Systems Sciences, and Engineering, Lecture Notes in Electrical Engineering 152*, pages 227–239, 2013.

[55] Takahashi, T; Kadobayashi, Y; Fujiwara, H. Ontological Approach toward Cybersecurity in Cloud Computing Categories and Subject Descriptors. In *Proceedings of the 3rd international conference on Security of information and networks*, pages 100–109, Taganrog, Russian Federation, 2010.

[56] Tsoumas, B; Dritsas, S; Gritzalis, D. An Ontology-Based Approach to Information Systems Security Management. In *Proceedings of the Third International Workshop on Mathematical Methods, Models, and Architectures for Computer Network Security, MMM-ACNS 2005*, pages 151–164, St. Petersburg, Russia, 2005.

[57] Tsoumas, B; Gritzalis, D. Towards an Ontology-based Security Management. In *20th International Conference on Advanced Information Networking and Applications - Volume 1 (AINA'06)*, pages 985–992, Washington, DC, 2006.

[58] von Solms, S. H; von Solms, R. *Information Security Governance*. New York: Springer Science+Business Media, LLC, 2009.

[59] Vorobiev, A; Bekmamedova, N. An Ontological Approach Applied to Information Security and Trust. In *Proceedings of the 18th Australasian Conference in Information Systems (ACIS 2007)*, pages 865–874, Toowoomba, Australia, 2007.

[60] Vorobiev, A; Bekmamedova, N. An Ontology-Driven Approach Applied to Information Security. *J. Res. Pract. Inf. Technol.* 42(1): 61–76, 2010.

[61] Vorobiev, A; Han, J; Bekmamedova, N. An Ontology Framework for Managing Security Attacks and Defences in Component Based Software Systems. In *Procedeeings of the 19th Australian Conference on Software Engineering, ASWEC 2008.*, pages 552–561, Perth, Australia, 2008.

[62] Vorobiev, A; Han, J. Security Attack Ontology for Web Services. In *Second International Conference on Semantics, Knowledge and Grid, pages* 42–48, Guilin, Guangxi, China, 2006.

[63] Wali, A; Chun, S. A; Geller, J. A Bootstrapping Approach for Developing a Cyber-security Ontology Using Textbook Index Terms. In *Proceedings of the 2013 International Conference on Availability, Reliability and Security*, pages 569–576, Regensburg, Germany, 2013.

[64] Wang, J. A; Guo, M. OVM: An Ontology for Vulnerability Management. In *Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence Research: Cyber Security and Information Intelligence Challenges and Strategies*, pages 1–4, Knoxville, Tennessee, 2009.

[65] Wang, J. A; Guo, M. Security Data Mining in an Ontology for Vulnerability Management. In *Proceedings of the International Joint Conference on Bioinformatics, Systems Biology and Intelligent Computing*, pages 597–603, Shanghai, China, 2009.

[66] Whitman, M. E; Mattor, H. J. *Principles of Information Security, Fourth Edition*. Course Technology, Cengage Learning, Boston, Massachusetts, 2012.

[67] Xu, H; Xiao, D; Wu, Z. Application of Security Ontology to Context-Aware Alert Analysis. In *Proceedings of the 2009 Eighth IEEE/ACIS International Conference on Computer and Information Science*, pages 171–176, Shanghai, China, 2009.

[68] Youseff, L; Butrico, M; Da Silva, D. Toward a Unified Ontology of Cloud Computing. In *Proceedings of the 2008 Grid Computing Environments Workshop*, pages 1–10, Austin, Texas, 2008.