ARES 2008

The Third International Conference on Availability, Security and Reliability

PROCEEDINGS

March 4-7, 2008 Barcelona, Spain

Edited by Stefan Jakoubi, Simon Tjoa, and Edgar R. Weippl

Organised by

[SECURE] Business Austria

DEXA

In cooperation with

UNIVERSITAT POLITÈCNICA DE CATALUNYA

enisa European Network and Information Security Agency

OESTERREICHISCHE COMPUTER GESELLSCHAFT AUSTRIAN COMPUTER SOCIETY

Proceedings of the

The Third International Conference on Availability, Security, and Reliability

March 4-7, 2008, Barcelona, Spain

CPS

Los Alamitos, California

Washington • Tokyo

IEEE computer society

IEEE Computer Society Order Number P3102
ISBN 0-7695-3102-4
ISBN 978-0-7695-3102-1
Library of Congress Number 2007909935

Additional copies may be ordered from:

IEEE Computer Society
Customer Service Center
10662 Los Vaqueros Circle
P.O. Box 3014
Los Alamitos, CA 90720-1314
Tel: + 1 800 272 6657
Fax: + 1 714 821 4641
http://computer.org/cspress
csbooks@computer.org

IEEE Service Center
445 Hoes Lane
P.O. Box 1331
Piscataway, NJ 08855-1331
Tel: + 1 732 981 0060
Fax: + 1 732 981 9667
http://shop.ieee.org/store/
customer-service@ieee.org

IEEE Computer Society
Asia/Pacific Office
Watanabe Bldg., 1-4-2
Minami-Aoyama
Minato-ku, Tokyo 107-0062
JAPAN
Tel: + 81 3 3408 3118
Fax: + 81 3 3408 3553
tokyo.ofc@computer.org

Individual paper REPRINTS may be ordered at: <reprints@computer.org>

Editorial production by Bob Werner
Cover art production by Joe Daigle/Studio Productions
Printed in the United States of America by The Printing House

IEEE computer society

CPS Conference Publishing Services

IEEE Computer Society
***Conference Publishing Services* (CPS)**
http://www.computer.org/cps

Table of Contents

The Third International Conference on Availability, Reliability and Security (ARES 2008)

Session 3: Models

Session 4: Database

Session 5: Mobile

Session 6: RBAC and Recommender

Session 7: Risk Management

Session 8: Networks

Session 9: Software

Session 4: Networks

Session 5: Crypto

Session 6: Crypto and Health

Session 7: Models and Networks

Session 8: IDS

Session 9: Hardware

Workshop FARES

Session 1: Miscellaneous

Session 2: Access Control and Algorithms

Session 3: Crypto

Session 4: Risk Management

Workshop PSAI

Workshop APE

Workshop SECSE

Workshop DAWAM

Workshop WAIS

Workshop WSDF

Workshop SREIS

Chair's Message

The Third International Conference on Availability, Reliability and Security (ARES 2008 – The International Dependability Conference) brings together researchers and practitioners in the area of dependability. ARES 2008 highlights the various aspects of dependability, with special focus on the crucial linkage between availability, reliability and security.

ARES aims at a full and detailed discussion of research issues in the field of dependability as an integrative concept that covers amongst others availability, safety, confidentiality, integrity, maintainability and security and their different areas of applications.

This conference emphasizes the interplay between foundations and practical issues of dependability in areas such as information systems, e-government, m-government, location-based services, ubiquitous computing, and autonomous computing.

This years ARES conference is devoted to the critical examination and research challenges of the various aspects of Dependable Computing and the definition of a future road map.

We are very happy to welcome three well-known keynote speakers:

- Prof. Ravi Sandhu (Executive Director, Institute for Cyber-Security Research (ICSR) and Lutcher Brown Endowed Chair in Cyber-Security, University of Texas, San Antonio)
- Prof. Vijay Atluri (Management Science and Information Systems Department, Rutgers University)
- Prof. Günther Pernul (Department of Information Systems, University of Regensburg)

From over 200 submissions we have selected the 44 best for a presentation as full paper. In addition, several workshops and short papers show ongoing research projects and offer interesting starting points for discussions.

We wish all participants an enjoyable conference and interesting discussions.

Edgar R. Weippl, Secure Business Austria, Vienna University of Technology

Gerald Quirchmayr, University of Vienna and University of South Australia

Jill Slay, University of South Australia

Conference Officers

Honorary Co-Chairs
Roland Wagner, University of Linz, Austria

General Co-Chairs
Guenther Pernul, University of Regensburg, Germany
Makoto Takizawa, Tokyo Denki University, Japan

Program Co-Chairs
Gerald Quirchmayr, University of South Australia, Australia
Jill Slay, University of South Australia, Australia
Edgar Weippl, Vienna University of Technology / Secure Business Austria, Austria

Workshops Co-Chairs
Leonard Barolli, Fukuoka Institute of Technology (FIT), Japan
A Min Tjoa, Vienna University of Technology, Austria

Organizing Chair
Fatos Xhafa, Technical University of Catalonia, Spain

International Liaison Co-Chairs
Maria Wimmer, University of Koblenz-Landau, Germany
Charles Shoniregun, University of East London, United Kingdom

Publicity Chair
Vladimir Marik, Czech Technical University, Czech Republic

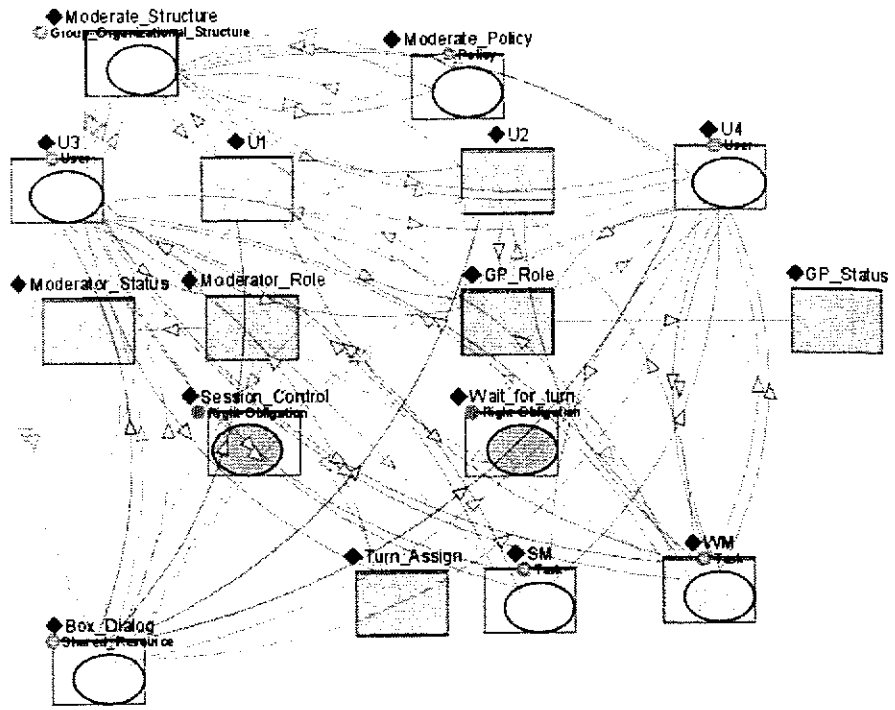

Figure 3. Ontology instances: Moderate policy. Figure generated by Jambalaya [13] plug-in for Protégé [14].

6. Conclusions

In this paper, we have presented policy-based group organizational structure management using an ontological approach. On the one hand, the policy-based approach dynamically adapts the behaviour of the group organizational structure without changing code and without requiring the consent or cooperation of the components being governed. On the other hand, the ontology-based policy specification, simplify the access to policy information, with the possibility of dynamically calculating relations between policies and environment, or entities based on ontology relations.

7. References

[1]. S. Wright, R. Chadha, G. Lapiotis (eds.), "Special Issue on Policy based Networking". IEEE Network, Vol. 16-2, 2002, pp. 8-56.

[2]. N. Damianou, N. Dulay, E. Lupu, M. Sloman, "The Ponder Policy Specification Language", Springer-Verlag, LNCS Vol. 1995, 2001, pp. 18-38.

[3]. J.M. Bradshaw, P. Beautement, L. Bunch, S. V. Drakunov et al., "Making Agents Acceptable to People". In N. Zhong, J. Liu (eds): Handbook of Intelligent Information Technology. IOS Press, 2003.

[4]. G. Tonti, J.M. Bradshaw, R. Jeffers, R. Montanari, N. Suri, and A. Uszok, "Semantic Web Languages for Policy Representation and Reasoning: A Comparison of KAoS, Rei, and Ponder", Springer-Verlag, LNCS Vol. 2870, 2003, pp. 419-437.

[5]. T.R. Gruber, "Toward principles for the design of ontologies used for knowledge sharing", International Journal of Human Computer Studies Vol. 43(5/6), 1995, pp. 907–928.

[6]. M. Uschold, and M. Gruninger, "Ontologies and Semantics for Seamless Connectivity", In SIGMOD Record, Vol. 33-4, 2004, pp. 58-4.

[7]. http://www.w3.org/2004/OWL/. OWL Web Ontology Language Guide.

[8]. http://www.w3.org/XML/.

[9]. http://www.w3.org/RDF/.

[10]. Online at: http://protege.stanford.edu/

[11]. H. Shen, P. Dewan, "Access Control for Collaborative Environments", In Proceedings CSCW of ACM, ACM Press, 1992, pp. 51–58.

[12]. C.A. Ellis, and S.J. Gibbs, "Concurrency control in groupware systems", "in proceedings ACM SIGMOD International Conference on Management of Data", 1989, pp. 399-407.

[13]. H.P. Dommel, J.J. Garcia-Luna-Aceves, "Floor Control for Multimedia Conferencing and Collaboration, ACM Multimedia, Vol. 5-1, 1997, pp. 23–38.

[14]. http://www.thechiselgroup.org/jambalaya

A Systematic Review and Comparison of Security Ontologies

Carlos Blanco[1], Joaquín Lasheras[2], Rafael Valencia-García[2], Eduardo Fernández-Medina[1], Ambrosio Toval[2] and Mario Piattini[1]

(1) Department of Information Technologies and Systems. University of Castilla-La Mancha
Paseo de la Universidad, 4. 13071. Ciudad Real (Spain)
{Carlos.Blanco, Eduardo.Fdzmedina, Mario.Piattini}@uclm.es
(2) Department of Informatics and Systems. University of Murcia
Campus Universitario de Espinardo. 30011. Murcia (Spain)
{jolave, valencia, atoval}@um.es

Abstract

The use of ontologies for representing knowledge provides us with organization, communication and reusability. Information security is a serious requirement which must be carefully considered. Concepts and relations managed by any scientific community need to be formally defined and ontological engineering supports their definition. In this paper, the method of systematic review is applied with the purpose of identifying, extracting and analyzing the main proposals for security ontologies. The main identified proposals are compared using a formal framework and we conclude by stating their early state of development and the need of additional research efforts.

1. Introduction

An ontology is a specification of a conceptualization [1]. It represents knowledge in a formal and structured form as well as provides a better communication, reusability and organization of knowledge and a better computational inference [2-4]. In this way, the main objective of ontologies is that of establishing ontological agreements not only to decrease language ambiguity but also to serve as a basis for communication between agents.

Information security is a serious requirement which must be carefully considered, not as an isolated aspect, but as an element presented in all stages of the development lifecycle, from requirement analysis to implementation and maintenance [5-7]. In this way, information assurance, security and privacy have moved from being considered by information systems designers as narrow topics of interest to become critical issues of fundamental importance in our society [8]. Some authors indicate that the survival of organizations depends on the correct management of information security and confidentiality [9].

It is very important to have the concepts and relations shared by the community formally defined. Therefore, several authors have indicated that the security community needs an ontology [10, 11] and they have considered this need as an important challenge and a research branch [7].

In this paper, we will carry out a systematic review of the existing literature on ontological engineering applied to security with the objective of knowing, analyzing and comparing the most relevant proposals. To perform this systematic review, we rely on the guideline proposed by Kitchenham [12] that is appropriate for software engineering researchers. In addition, we use a review protocol template developed by Biolchini [13] which facilitates systematic reviews planning and execution in software engineering.

The rest of the paper is organized as follows: in section 2, we will plan the review by defining the research question. Section 3 will execute the review and the first studies will be explained. Next, in section 4 we will define the data to be extracted and a data synthesis of the most relevant studies will be presented. In section 5, we will compare the ontologies and the results will be stated. Lastly, our conclusions will be set out in section 6.

2. Review Planning

In this phase, we must define the research objectives and the way in which the review will be executed

0-7695-3102-4/08 $25.00 © 2008 IEEE
DOI 10.1109/ARES.2008.33

which includes, both the formulations of research questions and the planning of how the sources and studies selection will be carried out.

2.1. Question Formularization

In this section, the research objectives must be clearly defined. The *question focus* is to identify the most relevant works centered in the development of ontologies that deal with security issues.

In section 1, we have presented not only security as a relevant aspect to be taken into account in the development process but also the ontologies being considered as a tool that provides us with advantages such as concepts unification of a community. In this way, our *problem* is the study of the existing proposals in ontological engineering applied to information security.

The *research question* which will be addressed by our research is the following one: What initiatives have been carried out to develop security ontologies in the field of ontological engineering? The *keywords and related concepts* that make up this question and that will be used during the review execution are:

- Ontology (Ontological Engineering), OWL, RDF, DAML.
- Security (Secure) and Privacy.

In the context of the planned systematic review, the security ontologies proposals will be *observed*, analyzed and compared. And therefore, the *population* group that will be observed is formed by publications in the selected data sources.

The expected *result* at the end of this systematic review is the identification of initiatives related to security ontologies. Additionally, the *outcome measures* are the number of identified initiatives grouped by area and the main comparison proposal. The main *application* area that will benefit from the systematic review results is the ontological engineering applied to the security, specifically academics, researchers or professionals interested in this field.

2.2. Sources Selection

The objective of this section is to select the sources where searches for primary studies will be executed.

The *selection criteria* to evaluate studies sources are based on the opinion of the authors of this work as experts in both ontological and security engineering. Besides, these sources must be web available and must possess search engines using keywords. The studies must be written in English. The following list of *sources* has been considered: ScienceDirect, ACM digital library, IEEE digital library, Scholar Google and DBLP. Later, the experts will refine the results and will include important works that had not been recovered in these sources.

2.3. Studies Selection

Once the sources are defined, it is necessary to describe the process and the criteria for studies selection and evaluation.

The *procedure* for studies selection consists of adapting our search chain to the syntax of each search engine and executing it. We then obtain a set of results to which the inclusion criteria is applied in order to obtain the relevant studies. Finally, the exclusion criteria is applied to the set of relevant studies in order to obtain our set of primary studies.

The studies *inclusion and exclusion criteria* are based on the research question, by finding proposals that make contributions to security ontological engineering. The inclusion criteria are focused on analyzing titles, keywords and abstracts of the studies, while the exclusion criteria mainly analyze abstracts, conclusions and other sections.

3. Review Execution

During this phase, the search in the defined sources must be executed and the obtained studies must be evaluated according to the established criteria. In next section, the information relevant to the research question must be extracted from the selected studies. The obtained studies which completely fit all previously defined inclusion and exclusion criteria are the following ones:

- Amaral et al. "An Ontology-based Approach to the Formalization of Information Security Policies" [14].
- Denker et al. "Security in the Semantic Web using OWL" [8].
- Denker et al. "Security for DAML Web Services: Annotation and Matchmaking" [15].
- Dobson et al. "Revisiting Ontology-Based Requirements Engineering in the age of the Semantic Web" [2].
- Donner. "Toward a Security Ontology" [10].
- Fenz et al. "Ontology based IT-security planning" [16].
- Firesmith. "A Taxonomy of safety-related requirements" [17].
- Geneiatakis et al. "An ontology description for SIP security flaws" [18].
- Giorgini et al. "Modelling Security and Trust with Secure Tropos" [19].
- Kagal et al. "Modeling conversation policies using permissions and obligations" [20].
- Karyda et al. "An ontology for secure e-government applications" [21].
- Kim et al. "Security Ontology for Annotating Resources" [22].
- Kwon et al. "Visual modelling and formal specification of constraints of RBAC using semantic web technology" [23].
- Lee et al. "Building Problem Domain Ontology from Security Requirements in Regulatory Documents" [24].
- Maamar et al. "Towards an ontology-based approach for specifying and securing Web services" [25].
- McGibney et al. "A service-centric model for intrusion detection in next-generation networks" [26].
- Mouratidis et al. "Integrating Security and Software Engineering: An Introduction" [7].
- Mouratidis et al. "An Ontology for Modelling Security: The Tropos Approach" [27].
- Raskin et al. "Ontology in information security: a useful theoretical foundation" [28].
- Tan et al. "Dynamic security reconfiguration for the semantic web" [29].
- Thuraisingham. "Security standards for the semantic web" [30].
- Tsoumas et al. "Towards an Ontology-based Security Management" [11].
- Undercoffer et al. "Modeling Computer Attacks: An Ontology for Intrusion Detection" [31].
- US Department of Defense. "Orange Book" [32].
- Vorobiev et al. "Security Attack Ontology for Web Services" [33].
- Yu et al. "A Social Ontology for Integrating Security and Software Engineering" [34].
- Zhou et al. "Ontology Based Software Reliability Modelling" [35].
- Zhou et al. "An Integrated QoS-Aware Service Development and Management Framework" [36].

4. Information Extraction

Once primary studies are selected, the extraction of relevant information begins. In this section, extraction criteria and results will be described.

To standardize the way that information will be represented we create forms to collect data from the selected studies. The information forms defined for this review are composed of three components: basic information (title, publication, authors and reference in EndNote format), general description (study area and summary) and our general impressions and comments. The selected areas to classify studies are as follows: security ontologies (general and applied to specific domain), theoretical works and semantic web oriented.

Next, we will present a brief outline of each of the selected studies in the previous section according to the extracted information obtained through the information forms. We will only focus on security ontologies proposals due to space constraints.

Denker et al. "Security in the Semantic Web using OWL" [8] and "Security for DAML Web Services: Annotation and Matchmaking" [15].

Authors develop several ontologies for security annotations of agents and web services, in a first work using DAML (DARPA Agent Markup Language) [15] and later using OWL (Web Ontology Language) [8]. These ontologies represent well-known security concepts and enable us to interconnect security standards. The defined ontology is formed by two sub-ontologies: "security mechanisms" that captures high-level security notations and "credential" that defines authentication methods.

Dobson et al. "Revisiting Ontology-Based Requirements Engineering in the age of the Semantic Web" [2].

Due to the emergence of the semantic web, the interest in ontologies is increasing. In this work, authors focus on the field of dependability requirements and revise ontologies for Requirements Engineering. They also define in OWL a dependability ontology compliant with the IFIP Working Group 10.4 taxonomy that includes security issues such as "dependability", "reliability", "availability", "integrity", "confidentiality" or "safety".

Fenz et al. "Ontology based IT-security planning"[16].

In this proposal, authors study security in small and medium size enterprises (SMEs) and propose a holistic solution based on a security ontology that includes low-cost risk management and threat analysis. The security ontology consists of five sub-ontologies. "Threat" is the main sub-ontology and includes proper countermeasures, threatened infrastructures and proper evaluation methods. "Attribute" sub-ontology models the impact of threats, "Infrastructure" describes infrastructure elements, "Role" maps enterprise

hierarchies and "Person" represents natural persons who are relevant for security issues modelling.

Firesmith "A Taxonomy of safety-related requirements" [17].

Firesmith states that the main objective of a safety engineer is that of identifying the requirements to keep valuable assets (like staff, property or environment) off threats. Ontologies could be used due to the fact that safety-related requirements typically have reuse potentials. He presents the following taxonomy of safety-related requirements: "Safety requirements" are requirements obtained from threats analysis. "Safety-significant requirements" includes non-safety requirements that can cause hazards and safety incidents. "Safety constraints" are constraints that directly impact safety and are derived from laws, policies, standards and industrial practices. "Safety system requirements" specify aspects of the primary system.

Karyda et al. "An ontology for secure e-government applications" [21].

In this work, the authors use OWL to propose a security ontology with which to develop secure applications. It captures the security knowledge of experts to support the communication between security experts, users and developers and developers use it to include security requirements as well as to support design choices.

The proposed ontology is formed of "assets" (data asset, hardware data,...), "countermeasures" (identification and authentication, network management, auditing services, physical protection,...), "objectives", "persons" (insider stakeholder, attacker,...) and "threats" (errors, attacks, technical failures,...). They validate the defined ontology using nRQL queries and in order to demonstrate that their ontology can be used in various contexts they apply it to e-government scenarios: e-tax and e-voting.

Kim et al. "Security Ontology for Annotating Resources" [22].

Authors use OWL for developing the NRL security ontology focused on annotation of functional aspects of resources. This ontology is capable of representing security statements like mechanisms, protocols, algorithms and credentials and can be applied to any electronic resource.

NRL presents an architecture easy to use and easy to extend, and is composed of seven sub-ontologies. Three of them are based on existing ontologies in DAML: firstly, "Service security ontology" that describes security annotation of semantic web services, secondly, "Agent security ontology" that enables querying of security information and finally "Information object ontology" that describes security of input and output parameters of web services.

The four remaining ontologies are as follows: "Main security ontology" that describes security protocols, mechanisms and policies, "Credentials ontology" that specifies authentication credentials, "Security algorithms ontology" that describes various security algorithms and "Security assurance ontology" that specifies different assurance standards.

Lee et al. "Building Problem Domain Ontology from Security Requirements in Regulatory Documents" [24].

In this paper, authors identify security requirements for certification and accreditation activities which are expressed in regulatory documents. These requirements have a non-functional nature that imposes complex constraints on behaviour of software systems and makes them hard to understand, predict and control.

Authors present a framework that includes techniques extracted from software requirements engineering and knowledge engineering and they propose a common language for extracting concepts from regulatory documents. They apply this methodology to build problem domain ontology from regulatory documents enforced by the DITSCAP - Department of Defense Information Technology Security Certification and Accreditation Process.

Mouratidis et al. "An Ontology for Modelling Security: The Tropos Approach" [27] and "Modelling Security and Trust with Secure Tropos" [19].

The Tropos methodology considers two approaches in software development: a security-oriented process and a management of the dependability-oriented process.

This methodology is based on social hierarchies and adapts components of the i* framework [34]. Authors improve the social ontology created for i* framework with new security concepts: constraints, secure entities (goals, tasks and secure resources) and secure dependences between actors.

Tsoumas et al. "Towards an Ontology-based Security Management" [11].

In this proposal, authors define security ontology in OWL and present a security framework of an arbitrary information system which provides security acquisition and knowledge management. They extend the DMTF Common Information Model (CIM) standard with

ontological semantics in order to use it as a container for IS security-related information.

Undercoffer et al. "Modeling Computer Attacks: An Ontology for Intrusion Detection" [31].

Here, first of all, authors analyzed around 4000 vulnerabilities and their exploit strategies and after that they created an ontology, in DAML+OIL and DAMLJessKB, for specifying computer attacks. In this paper, authors also summarize the main languages for specifying computer attacks: P-Best, STATL, LogWeaver, CISL, BRO, Snort Rules and IDMEF and present several use case scenarios with common attacks: "Denial of Service – Syn Flood", "The Classic Mitnick Type Attack" and "Buffer Overflow Attack".

Zhou et al. "An Integrated QoS-Aware Service Development and Management Framework" [36].

This work proposes a method for management and service quality assurance (QoS-aware) that consists of QoS-aware service management infrastructure, QoS ontology and QoS property ontology.

The QoS ontology provides us with a knowledge mapping with QoS concepts and relations that can be used for QoS-aware services communicating and exchanging. The QoS property ontology has two sub-obtologies: "Technical QoS property", that defines concepts and relations related to software development and "Managerial QoS property" focused on service providing.

Zhou et al. "Ontology Based Software Reliability Modelling" [35].

Authors propose an ontology-based method for software reliability modeling that includes a software reliability ontology developed in OWL together with an ontology-based software modeling system.

They describe reliability engineering as a series of interrelated processes by which reliability knowledge is reorganized with the support of methods, tools, models, organization, and the specifications of input and output.

In future works, they will focus on extending reliability ontology and applying the method to software architecture design.

5. Result Analysis

After the systematic review execution, the results must be summarized and analyzed using the methods defined during the planning phase. In this section, we classify the primary studies into the above defined areas and compare the main proposals to an ontological framework.

In Table 1, we present the primary studies classified by area and we observe that the greater part of the studies are security ontologies applied to specific domains.

Next, we compare the ontologies using a framework presented in [37], which is based on comparing basic elements (concepts, relations, attributes, etc) and measures made with OntoMetric framework [38]. It has not been possible to accomplish the comparison taking into consideration all the identified security ontologies because some of them are not web available and when we have tried to obtain them, authors have communicated us that their ontologies are still under construction.

In the following subsections, we present comparison results together with the conclusions that we have obtained after analyzing the available ontologies. These conclusions are shown by comparing similar ontologies: Denker versus Kim, which are general ontologies that describe secure mechanisms, and Dobson versus Undercoffer, which are focused on specific domains.

Table 1. Primary studies classified by area

Area	References	N° of studies
Security ontologies (general)	[8, 15, 21, 22, 24, 11, 36]	7
Security ontologies (applied to a specific domain)	[14, 2, 16-19, 27, 31, 34, 35]	10
Theoretical Works	[32, 10, 7, 28]	4
Semantic web-oriented	[8, 15, 20, 23, 25, 26, 29, 30, 33]	9

5.1. General Comparison

In Table 2, we present general measures of the available ontologies obtained using an OWL ontology editor, SWOOP.

Table 2. General comparison

	Denker	Kim	Dobson	Undercoffer
Number of concepts	87	82	92	106
Root concepts	45	20	32	41
Instances	136	81	61	22
Avg depth of inheritance	1,9	2,19	2,26	1,8
Avg of rel. concepts	0,57	0,37	0,62	0,55
Avg of attributes	0,11	0,42	1,18	0
Avg of subclasses	0,44	0,65	0,65	0,61
Number of taxonomic relations	42	62	60	65
Number of no taxonomic relations	24	25	25	75

We can observe that Denker's ontology has a greater number of concepts and instances than Kim's

proposal. This fact indicates that Kim's ontology is more general and does not detail any concrete area.

Kim's ontology is composed of seven sub-ontologies; one of them is focused on authentication methods and Denker defines it in greater depth. Denker performs a great conceptualization of the domain but he uses less attributes to define concepts and he should assign more properties as Kim does.

On the other hand, Dobson and Undercoffer proposals present a greater number of concepts because they try to model specific domains (dependability and computer attacks). Undercoffer neither identifies attributes nor use them for defining concepts.

The rest of our measures of this general comparison will be useful for the OntoMetric comparison accomplished in the following subsection.

5.1. OntoMetric

OntoMetric [38] is a method for comparing ontologies that is composed of factors grouped into five dimensions: represented contents, language, methodology, software environment and cost of using the ontology in new systems.

We focus on contents dimension that presents four factors: concepts, relations, concepts taxonomy and axioms. In relation to language dimension, all studied ontologies use OWL as representation language.

Every factor has measurable characteristics scored from 1 to 5 according to their low or high degree of accomplishment. The considered values for each characteristic will be shown in tables 3, 4, 5 and 6.

In table 3, we show the values for the concepts factor and we observe how Kim poorly describes concepts and does not formally specify them in natural language. On the contrary, Denker defines the concepts of the domain properly. Therefore, Kim's ontology makes its reutilization difficult because he does not describe concepts in natural language. However, Denker should assign more properties to each concept to correctly define the attributes that the concepts instances have.

Undercoffer's proposal is more difficult to understand because it poorly describes concepts, it does not make use of attributes to describe them and the used concepts identifiers are not representative. Nevertheless, Dobson widely describes concepts in natural language and includes attributes for defining them; therefore Dobson's ontology is more reusable.

In Table 4, we specify the values for the relations factor. In general, although relationships have been properly defined in the domain, they are not properly specified in natural language and not all of the formal properties of the relations are identified, in fact some authors such as Denker and Kim do not take them into account. They should specify relations in a formal way to obtain reusability and detection of incongruences.

Table 3. OntoMetric comparison: concepts factor

Concepts factor	Denker	Kim	Dobson	Undercoffer
Essential concepts	4	4	4	4
Essential concepts in superior levels	5	5	5	5
Concepts properly described in NL	2	1	3	1
Formal specification coincides with NL	4	4	4	4
Attributes describe concepts	1	1	2	2
Number of concepts	4	4	4	4

Table 4. OntoMetric comparison: relations factor

Relations factor	Denker	Kim	Dobson	Undercoffer
Essential relations	4	4	4	4
Relations relate appropriate concepts	5	5	5	4
Formal specification of relations coincides with naming	2	1	3	1
Arity specified	2	2	3	3
Formal properties of relations	1	1	2	2
Number of relations	4	4	4	5

Table 5. OntoMetric comparison: taxonomy factor

Taxonomy factor	Denker	Kim	Dobson	Undercoffer
Several perspectives	2	2	4	2
Appropriate not subclass of	1	1	1	1
Appropriate exhaustive partitions	2	4	3	4
Appropriate disjoint partitions	2	4	4	1
Maximum depth	3	4	4	3
Average of subclasses	3	3	3	3

Table 6. OntoMetric comparison: axioms factor

Axioms factor	Denker	Kim	Dobson	Undercoffer
Solve queries	2	2	3	3
Infer knowledge	2	3	3	4
Verify consistency	3	3	3	3
Not linked to concepts	2	3	1	1
Nº of axioms	1	1	3	3

The values for the taxonomy factor are presented in table 5. Kim and Denker do not use either several perspectives to classify the concepts or do not use the relation "not_subclass_of" to break an inheritance relation between concepts. Moreover, they could improve the use of appropriate exhaustive partitions by revising all possible decomposition classes in the domain. In the same way, Dobson and Undercoffer lack complete taxonomies.

In table 6, we show the axiom factor and its characteristics. Kim and Denker define few axioms and they cannot infer knowledge, only some restrictions to the value of the attributes of the concepts, while Dobson and Undercoffer use more constraints and can infer knowledge and verify consistency, but these are related to the concept of the ontology (they are not independent). It is advisable that authors include formal properties in the relations (reflexion, transitivity, asymmetry, symmetry and inverse function) which verify consistence.

6. Conclusions

In this section, we put forward our conclusions after planning the revision, executing it, analyzing primary studies and comparing the available proposals. We have observed that the greatest part of the identified works is focused on specific domains or the semantic web; therefore, we can affirm that so far, the scientific community has not accomplished a general security ontology but the need of security ontology has been identified as a branch of research.

Defining ontology is considered a main task within any scientific community; in this way, we give formal support and sharing capabilities to the managed knowledge. In the security field, it is impossible to formalize all existing concepts, so the definition of a complete security ontology is not an isolated task and the community should add efforts for joining and improving the developed ontologies. This complete security ontology should be flexible and easy to update for including changes along with new concepts that appear in the community.

In addition, we have observed how the greatest part of the selected works is still at the early stages of development and the source files of the security ontologies are not available yet for their study.

We have compared the available proposals and we have found out that not only include few attributes for defining concepts but also the natural language expressions used for describing them are not appropriate. They are not exhaustive because the ontologies do not define all possibilities of the studied domain, so we have identified this lack as a future work. These ontologies use few axioms and formal properties for inferring knowledge like reflexivity, transitivity, symmetry, asymmetry and inverse function.

We can conclude that the existing ontologies are not prepared for being reused and extended and that the security community still needs a complete security ontology that solves these lacks and provides reusability, communication and knowledge sharing.

In this sense, we have tried to combine the ontologies identified in section 5 but we have had some problems such as common concepts have different terms applied to them: for example, Kim specifies the terms CryptograhicKey and BiometricToken, while Denker uses Key and Biometric. Furthermore, we have identified deficiencies in the attributes associated to the ontology and in the use of some expressions in natural language for describing concepts so that to combine both ontologies has been impossible without being the creator of the ontologies and to know exactly what this term mean, although being a domain expert.

Acknowledgements

This research is part of the Projects ESFINGE (TIN2006-15175-C05-05), DEDALO (TIC2006-15175-C05-03) and RETISTRUST (TIN2006-26885-E) financed by the "Ministerio de Educación y Ciencia", and the MISTICO (PBC-06-0082) financed by the FEDER and the "Consejería de Ciencia y Tecnología de la Junta de Comunidades de Castilla-La Mancha (Spain)".

References

[1] Gruber, T., Towards Principles for the Design of Ontologies used for Knowledge Sharing. International Journal of Human-Computer Studies, 1995. 43(5/6): p. 907-928.

[2] Dobson, G. and P. Sawyer, Revisiting Ontology-Based Requirements Engineering in the age of the Semantic Web. International Seminar on "Dependable Requirements Engineering of Computerised Systems at NPPs", Institute for Energy Technology (IFE), Halden, 2006.

[3] Fernández-Breis, J.T. and R. Martínez-Béjar, A cooperative framework for integrating ontologies. International Journal of Human-Computer Studies, 2002. 56: p. 665-720.

[4] Gruninger, M. and J. Lee, Ontology Applications and Design. Communications of the ACM, 2002. 45(2): p. 39-41.

[5] Devanbu, P. and S. Stubblebine, Software engineering for security: a roadmap. ACM Press. Future of Software Engineering, 2000: p. 227-239.

[6] Ferrari, E. and B. Thuraisingham. Secure Databases Systems. in Advanced Databases: Technology Design. 2000. Artech Huse: London.

[7] Mouratidis, H. and P. Giorgini, An Introduction, in Integrating Security and Software Engineering: Advances and Future Visions. 2006, Idea Group Publishing.

[8] Denker, G., L. Kagal, and T. Finin, Security in the Semantic Web using OWL. Information Security Technical Report, 2005. 10(1): p. 51-58.

[9] Dhillon, G. and J. Backhouse, Information system security management in the new millennium. Communications of the ACM, 2000. 43(7): p. 125-128.
[10] Donner, M., Toward a Security Ontology. IEEE Security and Privacy, 2003.
[11] Tsoumas, B. and D. Gritzalis, Towards an Ontology-based Security Management. Proceedings of the 20th International Conference on Advanced Information Networking and Applications. IEEE Computer Society, 2006. Volume 1 (AINA'06) - Volume 01 AINA '06.
[12] Kitchenham, B., Procedures for performing systematic reviews (Joint Technical Report), in TR/SE-0401. 2004, Software Engineering Group. Department of Computer Science: Keele University. p. 33 p.
[13] Biolchini, J. and P. Gomes, Systematic Review in Software Engineering. 2005, Systems Engineering and Computer Science Department, UFRJ: Río de Janeiro, Brazil.
[14] Amaral, F.N.d., et al., An Ontology-based Approach to the Formalization of Information Security Policies. Proceedings of the 10th IEEE on International Enterprise Distributed Object Computing Conference Workshops EDOCW '06. IEEE Computer Society, 2006.
[15] Denker, G., et al., Security for DAML Web Services: Annotation and Matchmaking, in The SemanticWeb - ISWC 2003. 2003, Springer Berlin / Heidelberg. p. 335-350.
[16] Fenz, S. and E. Weippl, Ontology based IT-security planning. Proceedings of the 12th Pacific Rim International Symposium on Dependable Computing PRDC '06. IEEE Computer Society, 2006: p. 389-390.
[17] Firesmith, D., Engineering safety-related requirements for software-intensive systems, in Proceedings of the 27th international conference on Software engineering. 2005, ACM Press: St. Louis, MO, USA.
[18] Geneiatakis, D. and C. Lambrinoudakis, An ontology description for SIP security flaws. Computer Communications, 2006. In Press, Corrected Proof.
[19] Giorgini, P., H. Mouratidis, and N. Zannone, Modelling Security and Trust with Secure Tropos, in Integrating Security and Software Engineering: Advances and Future Visions. 2006, Idea Group Publishing.
[20] Kagal, L. and T. Finin, Modeling conversation policies using permissions and obligations. AAMAS workshop on Agent communication, LNCS. Springer-Verlag, 2005.
[21] Karyda, M., et al., An ontology for secure e-government applications. First International Conference on Availability, Reliability and Security (ARES'06). IEEE Computer Society, 2006: p. 1033-1037.
[22] Kim, A., J. Luo, and M. Kang. Security Ontology for Annotating Resources. in 4th International Conference on Ontologies, Databases, and Applications of Semantics (ODBASE'05). 2005. Agia Napa, Cyprus.
[23] Kwon, J. and C.-J. Moon, Visual modeling and formal specification of constraints of RBAC using semantic web technology. Knowledge-Based Systems, 2006. In Press, Corrected Proof.
[24] Lee, S.-W., et al., Building problem domain ontology from security requirements in regulatory documents, in Proceedings of the 2006 international workshop on Software engineering for secure systems. 2006, ACM Press: Shanghai, China.
[25] Maamar, Z., N.C. Narendra, and S. Sattanathan, Towards an ontology-based approach for specifying and securing Web services. Information and Software Technology, 2006. 48(7): p. 441-455.
[26] McGibney, J., N. Schmidt, and A. Patel, A service-centric model for intrusion detection in next-generation networks. Computer Standards & Interfaces, 2005. 27(5): p. 513-520.
[27] Mouratidis, H., P. Giorgini, and G. Manson, An Ontology for Modelling Security: The Tropos Approach, in Knowledge-Based Intelligent Information and Engineering Systems. 2003, Springer Berlin / Heidelberg. p. 1387-1394.
[28] Raskin, V., et al., Ontology in information security: a userful theoretical foundation. Proceedings of the 2001 workshop on New security paradigms NSPW'01. ACM Press, 2001.
[29] Tan, J.J. and S. Poslad, Dynamic security reconfiguration for the semantic web. Engineering Applications of Artificial Intelligence, 2004. 17(7): p. 783-797.
[30] Thuraisingham, B., Security standards for the semantic web. Computer Standards & Interfaces, 2005. 27(3): p. 257-268.
[31] Undercoffer, J., A. Joshi, and J. Pinkston. Modeling Computer Attacks: An Ontology for Intrusion Detection. in The Sixth International Symposium on Recent Advances in Intrusion Detection. 2003: Springer.
[32] DOD, Orange Book. Estándar DOD 5200.58-STD., in www.radium.ncsc.mil/tpep/library/rainbow/5200.28-STD.html, D.d.d.d.l. EEUU, Editor. 1970.
[33] Vorobiev, A. and J. Han, Security Attack Ontology for Web Services. Proccedings of the Second International Conference on Semantics, Knowledge, and Grid SKG '06. IEEE Computer Society, 2006: p. 42.
[34] Yu, E., L. Liu, and Mylopoulos, A Social Ontology for Integrating Security and Software Engineering, in Integrating Security and Software Engineering: Advances and Future Visions. 2006, Idea Group Publishing.
[35] Zhou, J., E. Niemelä, and A. Evesti, Ontology-based software reliability modelling. Proccedings of Software and Services Variability Management Workshop - Concepts, Models and Tools. Helsinki, Finland, 2007: p. 17-31.
[36] Zhou, J., E. Niemela, and P. Savolainen, An Integrated QoS-Aware Service Development and Management Framework. wicsa, 2007: p. 13.
[37] Blomqvist, E., A. Öhgren, and K. Sandkuhl. Ontology Construction in an Enterprise Context: Comparing and Evaluating Two Approaches. in In Proceedings of the Eighth International Conference on Enterprise Information Systems: Databases and Information Systems Integration. 2006. Paphos, Cyprus.
[38] Lozano-Tello, A. and A. Gómez-Pérez, ONTOMETRIC: A Method to Choose the Appropriate Ontology. Journal of Database Management. Special Issue on Ontological analysis, Evaluation, and Engineering of Business Systems Analysis Methods, 2004. 15(2).

Context Ontology for Secure Interoperability

Céline Coma[1], Nora Cuppens-Boulahia[1], Frederic Cuppens[1], Ana Rosa Cavalli[2]
[1] GET/ENST Bretagne, 2 rue de la chataigneraie, 35512 Cesson Sevigne Cedex, France
[2] GET/INT Evry-CNRS, 9, rue Charles Fourier, 91011 Evry, France

Abstract

During interoperability exchanges, organizations are ly conducting computation and sharing tasks. How- organizations can have different security policies. To ntee good interoperability exchanges, organizations to share with other participants information about the ices they provide. In addition, to be compliant with se- requirements during interoperability, security poli- have to be dynamic. One purpose of this paper is to ide this dynamic behavior by taking care about con- of access parameters. The context-aware security re- ments may be met by using a contextual access control el to define the security policy of each party involved e interaction, and OrBAC (Organization based Access rol) is an adequate model for this purpose. Elaborating ntology based security model provides a mean to ensure ing of understandable knowledge, in particular knowl- needed to derive the authorized accesses and usages ng the interoperability sessions. In this paper, we thus gest a context ontology to be combined with an ontologi- representation of the OrBAC model and show how it can sed to ease the security rules definition and derivation ng interoperability sessions.

words: *Security model, Interoperability, Ontology, ext, OrBAC*

ntroduction

he growth of the Internet has triggered opportunities cooperative computation and electronic interoperation teroperation), where enterprizes are jointly conducting putation and sharing business tasks based on the clas- resources they each supply or authorize to use or to ult. These e-interoperations generally occur between nizations having different security policies. To conduct interoperation, one organization must usually access sources of the other participants; however if no entity e trusted enough to access or modify all the resources hatever is the environment conditions (temporal, his- torical, spatial, etc.), context-aware access control is a primary concern. Moreover, support in the exchange of data, information, and knowledge is the key interoperation issue in current computer technology. Ontologies provide shared and common understanding of an application domain that can be communicated between organizations undertaking a collaboration. These ontologies play a major role in supporting secure e-interoperability. Most of current access control models do not support web semantics and ontologies to formally express security contexts and hence to ease the derivation of security rules in the case of interoperability. These ontologies are necessary to allow establishment of semantics compatibility between concepts used by organizations involved in a collaborative work. Semantics compatibility is needed to define or derive interoperation security policy used to accept or deny accesses.

We suggest in this paper a way to express collaborative contexts based on ontology definition and how they can be used to specify dynamic security policies. In Section 2, we analyze several contextual and ontology based access control models. Based on this analysis, we show that OrBAC [2, 14, 11] meets the requirements of flexibility and completeness we need to achieve our objectives. So we recall the main features of the OrBAC model in Section 3 and propose an ontological based description of OrBAC. In Section 4, we present our context taxonomy. Section 5 studies relationships between basic contexts. There are three types of relations: internal, composition and external. Definition of these relations and the preservation of ontology consistency are main challenges when creating our context ontology and defining security rules used to make access decisions. Section 6 presents ontological mapping which is used to define security policies of organizations that want to interoperate. In Section 7, we briefly show how to apply our approach in P2P collaboration. Finally, Section 8 concludes this paper.

2. Context and ontology in access control

Most access control models which take into account context are based on the R-BAC model [18]. Bertino *et al.* suggest extensions of R-BAC to take into account temporal

02-4/08 $25.00 © 2008 IEEE
09/ARES.2008.133

Author Index

The Third International Conference on Availability, Reliability and Security (ARES 2008)

Notes

IEEE Computer Society Conference Publications Operations Committee

IEEE Computer Society Publications

The world-renowned IEEE Computer Society publishes, promotes, and distributes a wide variety of authoritative computer science and engineering texts. These books are available from most retail outlets. Visit the CS Store at *http://www.computer.org/portal/site/store/index.jsp* for a list of products.

IEEE Computer Society *Conference Publishing Services* (CPS)

The IEEE Computer Society produces conference publications for more than 250 acclaimed international conferences each year in a variety of formats, including books, CD-ROMs, USB Drives, and on-line publications. For information about the IEEE Computer Society's *Conference Publishing Services* (CPS), please e-mail: cps@computer.org or telephone +1-714-821-8380. Fax +1-714-761-1784. Additional information about *Conference Publishing Services* (CPS) can be accessed from our web site at: *http://www.computer.org/cps*

IEEE Computer Society / Wiley Partnership

The IEEE Computer Society and Wiley partnership allows the CS Press *Authored Book* program to produce a number of exciting new titles in areas of computer science and engineering with a special focus on software engineering. IEEE Computer Society members continue to receive a 15% discount on these titles when purchased through Wiley or at: *http://wiley.com/ieeecs*. To submit questions about the program or send proposals, please e-mail jwilson@computer.org or telephone +1-714-816-2112. Additional information regarding the Computer Society's authored book program can also be accessed from our web site at:
http://www.computer.org/portal/pages/ieeecs/publications/books/about.html

Revised: 21 January 2008

CPS Online™

IEEE Online Collaborative Publishing Environment

CPS Online is our innovative online collaborative conference publishing system designed to speed the delivery of price quotations and provide conferences with real-time access to all of a project's publication materials during production, including the final papers. The ***CPS Online*** workspace gives a conference the opportunity to upload files through any Web browser, check status and scheduling on their project, make changes to the Table of Contents and Front Matter, approve editorial changes and proofs, and communicate with their CPS editor through discussion forums, chat tools, commenting tools and e-mail.

The following is the URL link to the ***CPS Online*** Publishing Inquiry Form:
http://www.ieeeconfpublishing.org/cpir/inquiry/cps_inquiry.html

Published by the IEEE Computer Society
10662 Los Vaqueros Circle
P.O. Box 3014
Los Alamitos, CA 90720-1314

IEEE Computer Society Order Number P3102
Library of Congress Number 2007909935
ISBN 0-7695-3102-4