Patrocinadores

Ministerio de Educación y Ciencia · Zaragoza Ayuntamiento · Ministerio de Industria, Turismo y Comercio · Universidad de Zaragoza · Sun · Telefónica · Expo Zaragoza 2008 · Gobierno de Aragón, Departamento de Ciencia, Tecnología y Universidad

Entidades Organizadoras

- AdaSpain.
- Asociación de Enseñantes Universitarios de la Informática (AENUI).
- Asociación de Técnicos Informáticos (ATI).
- Asociación Española para la Inteligencia Artificial (AEPIA).
- Asociación para la Interacción Persona-Ordenador (AIPO).
- Asociación para el Desarrollo de la Informática Educativa (ADIE).
- Ayuntamiento de Zaragoza.
- Capítulo Español de la IEEE Computational Intelligence Society.
- Comité Español de Automática (CEA).
- Conferencia de Decanos y Directores de Informática (CODDI) de las Universidades Españolas.
- Departamento de Informática e Ingeniería de Sistemas de la Universidad de Zaragoza.
- European Society for Fuzzy Logia and Technology (EUSFLAT).
- Federación de Asociaciones de Ingenieros en Informática (AI2).
- W3C España (World Wide Web Consortium).
- Programa Nacional de Tecnologías Informáticas - Dirección General de Investigación. Ministerio de Educación y Ciencia.
- Red Española de Metaheurísticas.
- Red Española de Minería de Datos y Aprendizaje.
- Sección Española de la European Association for Computer Graphics (EUROGRAPHICS).
- Sociedad de Arquitectura y Tecnología de Computadores (SARTECO).
- Sociedad de Ingeniería del Software y Tecnologías de Desarrollo del Software (SISTEDES).
- Universidad de Zaragoza.

ISBN: 978-84-9732-607-0

CEDI 2007 II Simposio sobre Seguridad Informática | SSI'07 |

THOMSON

CEDI 2007

II CONGRESO ESPAÑOL DE INFORMÁTICA

ZARAGOZA SPAIN

AUDITORIO PALACIO DE CONGRESOS
11 AL 14 DE SEPTIEMBRE DE 2007

II Simposio sobre Seguridad Informática

| SSI'07 |

EDITORES
Benjamín Ramos Álvarez y Arturo Ribagorda Garnacho

ACTAS DEL
II SIMPOSIO SOBRE SEGURIDAD INFORMÁTICA [SSI'2007]

EDITORES

Benjamín Ramos Álvarez
Arturo Ribagorda Garnacho

SIMPOSIO ORGANIZADO POR

Grupo de Seguridad de las Tecnologías de la Información (SeTI)
Universidad Carlos III de Madrid

Grupo de Tecnologías de las Comunicaciones (GTC)
Universidad de Zaragoza

ENTIDADES COLABORADORAS

ACTAS DEL II SIMPOSIO SOBRE SEGURIDAD INFORMÁTICA (SSI'07)

Magallanes, 25; 28015 Madrid, ESPAÑA
Teléfono 91 4463350
Fax: 91 4456218
clientes@paraninfo.es

ISBN: 978-84-9732-607-0
Depósito legal: M-

Maquetación: Los Editores
Coordinación del proyecto: @LIBROTEX
Portada: Estudio Dixi
Impresión y encuademación: FER Fotocomposición, S. A.

IMPRESO EN ESPAÑA-PRINTED IN SPAIN

Presidente

Arturo Ribagorda Garnacho
Universidad Carlos III de Madrid

Vicepresidente

Benjamín Ramos Álvarez
Universidad Carlos III de Madrid

Secretario

José Luis Salazar Riaño
Universidad de Zaragoza

Comité de programa

Abascal Fuentes, Policarpo	Universidad de Oviedo
Álvarez Marañón, Gonzalo	CSIC
Areitio Bertolín, Javier	Universidad de Deusto
Borrell Viader, Joan	Universidad Autónoma de Barcelona
Caballero Gil, Pino	Universidad de La Laguna
Cabello, Adán	Universidad de Sevilla
Curty Alonso, Marcos	Universidad de Zaragoza
Dávila Muro, Jorge	Universidad Politécnica de Madrid
Domingo-Ferrer, Josep	Universidad Rovira i Virgili
Estévez Tapiador, Juan	Universidad Carlos III de Madrid
Fernández-Medina Patón, Eduardo	Universidad de Castilla La Mancha
Ferrer Gomila, Josep Lluis	Universidad Illes Balears
Fúster Sabater, Amparo	CSIC
García Teodoro, Pedro	Universidad de Granada
Gómez Eskarmeta, Antonio	Universidad de Murcia
González-Tablas Ferreres, Ana Isabel	Universidad Carlos III de Madrid
González Jiménez, Santos	Universidad de Oviedo
González Vasco, María Isabel	Universidad Rey Juan carlos
Gutiérrez Gutiérrez, Jaime	Universidad de Cantabria
Hernández Castro, Julio César	Universidad Carlos III de Madrid
Hernández Encinas, Luis	CSIC
Hernández Goya, Candelaria	Universidad de La Laguna

Herrera Joancomartí, Jordi	UOC
Huguet Rotger, Llorenç	Universidad Illes Balears
López Muñoz, Javier	Universidad de Málaga
Malagón Poyato, Chelo	CSIC-RedIris
Mañas Argemí, José Antonio	Universidad Politécnica de Madrid
Martín del Rey, Ángel	Universidad de Salamanca
Melús Moreno, José Luis	Universidad Politécnica de Cataluña
Miret Biosca, Josep María	Universidad de Lleida
Munuera Gómez, Carlos	Universidad de Valladolid
Orfila Díaz-Pabón, Agustín	Universidad Carlos III de Madrid
Ortega García, Javier	Universidad Autónoma de Madrid
Padró Laimon, Carles	Universidad Politécnica de Cataluña
Peinado Domínguez, Alberto	Universidad de Málaga
Pérez González, Fernando	Universidad de Vigo
Ramió Aguirre, Jorge	Universidad Politécnica de Madrid
Ramos Álvarez, Benjamín	Universidad Carlos III de Madrid
Ribagorda Garnacho, Arturo	Universidad Carlos III de Madrid
Rifá Coma, Josep	Universidad Autónoma de Barcelona
Robles Martínez, Sergi	Universidad Autónoma de Barcelona
Salazar Riaño, José Luis	Universidad de Zaragoza
Sánchez Reíllo, Raúl	Universidad Carlos III de Madrid
Sempere Luna, José María	Universidad Politécnica de Valencia
Soriano Ibáñez, Miquel	Universidad Politécnica de Cataluña
Tena Ayuso, Juan	Universidad de Valladolid
Villar Santos, Jorge	Universidad Politécnica de Cataluña

Presentación

Hace dos años se celebró en Granada el primer CEDI (Congreso Español de Informática), lo que supuso un hito en nuestro país para las reuniones académicas de las numerosas materias que hoy en día engloba esta macrodisciplina que denominamos informática. Así pues, ésta fue la primera vez que gracias al esfuerzo coordinado de un gran número de profesores e investigadores –atinadamente dirigidos por los organizadores–, se logró reunir en un mismo escenario y en un breve lapso de tiempo a la práctica totalidad de los académicos que nos dedicamos a la informática.

Naturalmente, la seguridad de la información –una de las más pujantes disciplinas de la informática–, no podía estar ausente de este acontecimiento, y por ello celebramos en dicha ocasión el Simposio sobre Seguridad Informática. Esta participación fue una decisión fácil de tomar por parte de los que nos dedicamos a esta disciplina, pues aunque desde el ya lejano 1988 convocábamos una reunión bienal (de nombre Reunión Española de Criptología y Seguridad de la Información, más conocida como RECSI), no podíamos dejar pasar la oportunidad de acogernos al paraguas de CEDI y sumarnos a un Congreso que llamaba a todos nuestros compañeros y amigos de otras disciplinas hermanas.

Además, se da la circunstancia de que CEDI, aun siendo de periodicidad bienal, como RECSI, se reúne los años impares, mientras que la última lo hace los pares, por lo que aquél, aparte de su intrínseco interés, nos ofrecía a los dedicados a la seguridad la posibilidad de seguir manteniendo el contacto entre años impares.

Dado que la iniciativa fue un éxito, y en el 2005 el Simposio sobre Seguridad Informática congregó a un número importante de participantes, parecía indudable que se debía mantener la cita este año en Zaragoza, como así se hizo en su momento, con el resultado que este libro de actas muestra y que los lectores deben de juzgar.

Por lo que atañe a la seguridad de la información, cabe decir que es uno de los campos que ha experimentado en los últimos diez años un crecimiento más vertiginoso, principalmente en todo el llamado primer mundo.

En nuestro país, son tres las principales causas de este hecho. Por un lado, la rápida expansión de Internet, que en poco tiempo ha alcanzado todos los rincones de nuestra sociedad, convirtiéndose en una instrumento ineludible

para las empresas, sin el cual no ya su actividad, sino incluso su presencia entre sus clientes se veía seriamente comprometida. Igualmente, para las Administraciones Públicas Internet supone satisfacer los principios constitucionales de "eficacia, descentralización y coordinación", que, entre otros, deben guiar sus actuaciones, así como atender las demandas de los ciudadanos que requieren servicios públicos ágiles y accesibles.

En segundo lugar, la promulgación en el año 1992 de la Ley Orgánica de Regulación del Tratamiento Automatizado de Datos de Carácter Personal (LORTAD) – derogada en 1999 por la Ley Orgánica de Protección de Datos de Carácter Personal (LOPD)–, y sobre todo la publicación en 1999 del Real Decreto 994/1999 (Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal), supuso un revulsivo para empresas y Administraciones Públicas obligadas, so pena de ser sancionadas por la Agencia Española de Protección de Datos, a adoptar mecanismos y procedimientos de seguridad para proteger los datos personales que manejaban.

En tercer lugar, la presión de los usuarios informáticos, nada proclives a abandonar procedimientos ancestrales de relación con organismos públicos y privados, salvo que se les ofreciesen las mismas garantías de seguridad que se les supone (a menudo con más fe que raciocinio) a los procedimientos que se pretendían sustituir.

Por todo ello, lo que a finales de los ochenta era un pequeño grupo de académicos interesados casi en exclusiva por la criptología, ha devenido en un importante número de investigadores y docentes que, sin abandonar dicho campo, trabajan igualmente en los numerosos temas que figuran entre los de interés de este Simposio, y cuyas aportaciones se presentan en este libro.

Esperamos que estas actas y la reunión del próximo septiembre sirvan para potenciar aún más el interés y desarrollo de la seguridad, sin cuyo concurso difícilmente avanzaremos en la sociedad de la información que estamos conformando y de la que tanto esperamos para el progreso de la humanidad.

ÍNDICE

Criptografía

Autenticación y Biometría

Sistemas de detección y protección ante intrusos

Redes P2P y MANET

Gestión de la Seguridad

Protocolos y aplicaciones de seguridad

Ontologías de seguridad: revisión sistemática y comparativa

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

[1]Dept. de Tecnologías y Sistemas Informáticos
Escuela Superior de Informática
Universidad de Castilla-La Mancha
Paseo de la Universidad, 4
13001 Ciudad Real
{Carlos.Blanco, Eduardo.FdezMedina, Mario.Piattini}@uclm.es

[2]Dept. Informática y Sistemas
Facultad de Informática
Universidad de Murcia
Campus Universitario de Espinardo
30011 Murcia
{jolave, valencia, atoval}@um.es

Resumen

El uso de ontologías en la representación del conocimiento nos proporciona organización, comunicación y reutilización. El área de la seguridad, como otras muchas en ingeniería del software también necesita la definición de ontologías en las que se especifiquen los conceptos y relaciones que se manejan en la comunidad científica. En este trabajo aplicamos la técnica de revisión sistemática para realizar un estudio de las propuestas de ontologías de seguridad existentes y poder sacar conclusiones sobre la necesidad de seguir investigando en el desarrollo de una o varias ontologías de seguridad o por el contrario si se trata de un problema ya resuelto por la comunidad científica.

1. Introducción

Una ontología es una especificación explícita de una conceptualización [16] que nos permite una formalización en la representación del conocimiento mejorando su representación, organización, razonamiento, reutilización y compartición [8, 12, 17]. Los principales objetivos de las ontologías son la descripción de acuerdos ontológicos sirviendo como base para la comunicación entre agentes (sean humanos o software) y el filtrado de conocimiento ayudando a la construcción de metamodelos expresando lo que se debe o no incluir [30]. Existen varios lenguajes que nos permiten la representación de ontologías, principalmente OWL (Web Ontology Language), DAML (DARPA Agent Markup Language) y RDF (Resource Description Framework).

La importancia de la seguridad de la información queda de manifiesto en numerosos trabajos. En [7] aseguran que la supervivencia de las organizaciones depende de la correcta gestión de la seguridad y confidencialidad de la información. Debido a su importancia, no es correcto que la seguridad se considere de forma aislada sino como un elemento presente en todas las etapas del proceso de desarrollo [6, 13]. De esta forma, aspectos como la confiabilidad, seguridad y privacidad de la información han pasado de ser meros aspectos de interés para los diseñadores de sistemas de información convirtiéndose en aspectos críticos y de vital importancia para la sociedad [4].

Dentro de cualquier comunidad científica es muy importante tener definidos formalmente los conceptos y relaciones que se comparten. De este modo varios autores apoyan la necesidad de la definición de una ontología de seguridad [10, 33], identificándola como un área de investigación importante y un reto dentro de la comunidad de la ingeniería de seguridad [27].

En este artículo realizamos una revisión de la literatura existente con el objetivo de conocer las propuestas relevantes en el campo de la ingeniería ontológica aplicada a la seguridad, para ello utilizamos la técnica de revisión sistemática [22], basándonos en un protocolo formal [2].

El resto del artículo está organizado de la siguiente forma: en la sección 2 planificamos la revisión definiendo la pregunta de investigación para posteriormente en la sección 3 ejecutar la revisión sobre las fuentes seleccionadas y obtener los estudios primarios. En la sección 4 mostramos un resumen de la información extraída sobre las propuestas que analizaremos en más detalle la sección 5. Por ultimo en la sección 6 señalamos las conclusiones de este trabajo.

2. Planificación de la revisión

En esta sección planificamos la revisión identificando principalmente sus objetivos y restricciones, estableciendo las fuentes de búsqueda y detallando el protocolo y criterios para la selección de los estudios primarios.

2.1. Formulación de la pregunta

En esta sección se definen los objetivos de la revisión.

Definimos como *foco de la pregunta* la localización de trabajos centrados en el desarrollo de ontologías que traten aspectos de seguridad y realicen aportaciones relevantes en el área.

A continuación comentamos los factores que definen la *amplitud y calidad de la pregunta*.

En la sección de introducción quedó de manifiesto tanto la necesidad de considerar la seguridad de la información como un aspecto relevante que ha de estar presente en todo el proceso de desarrollo, como las utilidades y beneficios que proporciona el uso de ontologías en cuanto a la unificación de conceptos de una determinada comunidad. De este modo, el *problema* a tratar se define como el estudio de los trabajos realizados en el punto en el que se unen estas dos áreas, aplicándose la ingeniería ontológica al campo de la seguridad de la información.

La *pregunta de investigación* que conduce la revisión es la siguiente: ¿qué trabajos aplicados a la seguridad se han llevado a cabo en la ingeniería ontológica?. Las *palabras clave* y *conceptos relacionados* (indicados entre paréntesis) que se usarán en la ejecución de la revisión son:

- Ontology (Ontological engineering), OWL, RDF, DAML.
- Security (secure) y privacy.

En el contexto de esta revisión sistemática se van a *observar* las propuestas existentes sobre ontologías de seguridad, extrayendo y comparando las más importantes, siendo la *población* a analizar las publicaciones presentes en las fuentes de datos seleccionadas.

Los *resultados esperados* al finalizar esta revisión es la identificación de las propuestas en ontologías de seguridad. La *medida de salida* será el número de estudios localizados agrupados según el área en el que se centran y la comparación de las propuestas de ontologías de seguridad mediante un marco formal de comparación de ontologías. Los beneficiarios de esta revisión serán los académicos, investigadores o profesionales relacionados con la ingeniería ontológica aplicada a la seguridad así como los relacionados con alguno de los dos campos de forma independiente que estén interesados en conocer los trabajos relevantes que hayan tratado el problema de la seguridad de la información mediante el uso de ontologías.

2.2. Selección de fuentes

El *criterio* de selección de las fuentes donde se ejecutará la revisión está basado en la opinión de los autores de este trabajo en calidad de expertos tanto en ingeniería ontológica como en seguridad. A dichas fuentes se les exige accesibilidad vía web y la presencia de motores de búsqueda. El lenguaje de los estudios primarios será el inglés.

Se ha considerado la siguiente *lista de fuentes*: ScienceDirect, ACM digital library, IEEE digital library, Scholar Google y DBLP. Tras la ejecución en dichas fuentes se realizará un refinamiento por parte de los autores en el que se incluirán trabajos importantes que no hayan podido ser recuperados.

2.3. Selección de estudios

Una vez definidas las fuentes establecemos el proceso y los criterios para la selección de los estudios.

El *criterio de inclusión y exclusión* se basa en los objetivos definidos, localizando y eliminando los trabajos que no realizan aportaciones sobre seguridad dentro de la ingeniería ontológica. El criterio de inclusión se centra en el análisis del título, palabras clave y abstract, mientras que el de exclusión analiza principalmente el abstract y las conclusiones, profundizando en otras secciones según requiera cada trabajo.

El *procedimiento* para la selección de los estudios primarios consiste en adaptar la cadena de búsqueda a cada fuente, ejecutar la consulta y aplicar el criterio de inclusión sobre los resultados para obtener el conjunto de estudios relevantes a los cuales, a continuación, se les aplicará el criterio de exclusión de forma que obtengamos el conjunto de estudios primarios.

3. Ejecución de la revisión

Una vez planificada la revisión procedemos a su ejecución en las fuentes seleccionadas evaluando los estudios según el protocolo y los criterios de inclusión y exclusión definidos. Tras la ejecución se realizó una fase de refinado en la que se introdujeron a juicio de los expertos (autores de este trabajo) estudios importantes que no fueron obtenidos. A continuación mostramos una lista con los estudios primarios obtenidos:

- Geneiatakis et al. "An ontology description for SIP security flaws" [14].
- Kwon et al. "Visual modelling and formal specification of constraints of RBAC using semantic web technology" [23].
- 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].
- Thuraisingham. "Security standards for the semantic web" [32].
- Denker et al. "Security in the Semantic Web using OWL" [4].
- Tan et al. "Dynamic security reconfiguration for the semantic web" [31].
- Denker et al. "Security for DAML Web Services: Annotation and Matchmaking" [5].
- Donner. "Toward a Security Ontology" [10].
- Fenz et al. "Ontology based IT-security planning" [11].
- Karyda et al. "An ontology for secure e-government applications" [20].
- Vorobiev et al. "Security Attack Ontology for Web Services" [35].
- Amaral et al. "An Ontology-based Approach to the Formalization of Information Security Policies" [1].
- Raskin et al. "Ontology in information security: a useful theoretical foundation" [29].
- Kim et al. "Security Ontology for Annotating Resources" [21].
- Mouratidis et al. "An Ontology for Modelling Security: The Tropos Approach" [28].
- Tsoumas et al. "Towards an Ontology-based Security Management" [33].
- Dobson et al. "Revisiting Ontology-Based Requirements Engineering in the age of the Semantic Web" [8].
- Kagal el al. "Modeling conversation policies using permissions and obligations" [19].
- Undercoffer et al. "Modeling Computer Attacks: An Ontology for Intrusion Detection" [34].
- Giorgini et al. "Modelling Security and Trust with Secure Tropos" [15].
- Mouratidis et al. "Integrating Security and Software Engineering: An Introduction" [27].
- Yu et al. "A Social Ontology for Integrating Security and Software Engineering" [36].
- Departamento de defensa de los EEUU. "Orange Book" [9].

4. Extracción de información

Una vez identificados los estudios primarios realizamos una fase en la que extraemos la información relevante de cada trabajo en base a un *formulario*. En él almacenamos la identificación del estudio (título, publicación, autores y referencia en formato EndNote), una descripción general (área y resumen) y los aspectos a destacar (en el que se incluyen comentarios, figuras, etc).

Las áreas que hemos considerado para la clasificación de los trabajos son:

- Propuestas de seguridad tanto generales como aplicadas a un dominio concreto.
- Trabajos teóricos que refuerzan la importancia de las ontologías de seguridad.
- Estudios centrados en la seguridad en la web semántica tanto teóricos como propuestas específicas.

Existen numerosas propuestas de ontologías de seguridad relacionadas con la web semántica debido al especial interés que ha sufrido ésta en los últimos años. Por este motivo hemos considerado oportuno agrupar estos trabajos en una clase propia.

A continuación comentamos cada estudio en base a la información extraída. Debido a restricciones de espacio nos centraremos en los trabajos que proponen las ontologías de seguridad que en la siguiente sección compararemos mediante un marco formal.

4.1. Denker et al. "Security in the Semantic Web using OWL" [4] y "Security for DAML Web Services: Annotation and Matchmaking" [5]

Los autores desarrollan una ontología para realizar anotaciones seguras en servicios web. En primer lugar utilizaron DAML en [5] y posteriormente OWL en [4]. Representan conceptos de seguridad bien conocidos y su objetivo es proporcionar notaciones que permitan la interconexión entre estándares de seguridad. La ontología esta formada por dos subontologías principales: "Security Mechanisms" y "Credential".

4.2. Fenz et al. "Ontology based IT-security planning" [11]

Proponen una ontología de seguridad que permite a pequeñas y medianas empresas implementar una propuesta integral de seguridad en TI incluyendo análisis de riesgos de bajo coste y análisis de amenazas.

La ontología está formada por cinco subontologías: "attribute" con conceptos importantes para modelar el impacto de las amenazas; "threat" es la parte central y trata conceptos y relaciones referentes a las amenazas; "infrastructure" describe algunos elementos de infraestructura; "role" para representar la jerarquía de la empresa; y "person" lista de personas relevantes.

4.3. Karyda et al. "An ontology for secure e-government applications" [20]

Capturan el conocimiento de los expertos mediante una ontología de seguridad con el fin de ser usada por los desarrolladores para la toma de decisiones y la inclusión de requisitos de seguridad. Aplican la ontología a los escenarios "e-government" de pago de tasas y sistema de voto y la validan mediante consultas nRQL.

4.4. Kim et al. "Security Ontology for Annotating Resources" [21]

Ontología de seguridad enfocada en la representación de aspectos funcionales. Se compone de las siguientes siete subontologías (de las cuales las tres últimas están basadas en ontologías existentes en DAML): "main security" describe conceptos de seguridad como protocolos, mecanismos o políticas; "credentials" especifica credenciales de autenticación; "security algorithms" algoritmos de seguridad; "security assurance" estándares para garantizar la seguridad; "service security" anotación de servicios web; "agent security" permite consultar la información de seguridad asociada al recurso; e "information object" que describe la seguridad asociada a los parámetros de entrada y salida de servicios web.

4.5. Mouratidis et al. "An Ontology for Modelling Security: The Tropos Approach" [28] y "Modelling Security and Trust with Secure Tropos" [15]

Extienden Tropos (*http://www.troposproject.org*) introduciendo nuevos conceptos que permiten modelar aspectos de seguridad. Describen la integración de dos enfoques, uno que proporciona un proceso orientado a la seguridad y otro que proporciona un proceso de gestión de la confiabilidad de los resultados.

Está inspirada en estructuras sociales y organizacionales representadas mediante el marco de modelado i* cuyos conceptos principales son actores, objetivos, tareas, recursos y dependencias. Para el marco i* también se ha descrito una ontología social [36], siendo los trabajos descritos en esta sección una extensión del i* para cubrir necesidades específicas del modelado y análisis de la seguridad.

Los conceptos de seguridad introducidos son: restricciones de seguridad, entidades seguras (objetivos, tareas y recursos seguros) y dependencias seguras entre actores.

4.6. Tsoumas et al. "Towards an Ontology-based Security Management" [33]

Presentan un marco para la adquisición y gestión del conocimiento referente a la seguridad en sistemas de información basado en una ontología de seguridad.

El almacenamiento de la información relacionada con la seguridad se realiza mediante la extensión del estándar DMTF "Common Information Model" (CIM) enriqueciéndolo con semántica ontológica para poder compartir y

reutilizar la ontología de seguridad definida en OWL.

4.7. Dobson et al. "Revisiting Ontology-Based Requirements Engineering in the age of the Semantic Web" [8]

Analizan el panorama de la ingeniería de requisitos enfocada desde el punto de vista de las ontologías, considerando el auge de la web semántica.

Proponen una "dependability ontology" en OWL que incluye aspectos de seguridad como "dependability", "reliability", "availability", "integrity", "confidentiality" o "safety".

4.8. Undercoffer et al. "Modeling Computer Attacks: An Ontology for Intrusion Detection" [34]

Tras analizar unas 4000 vulnerabilidades y las estrategias correspondientes utilizadas por los atacantes para explotarlas, desarrollan una ontología en DAML+OIL para especificar los modelos de ataque.

5. Análisis de resultados

Una vez ejecutada la revisión y estudiados los principales trabajos, en esta sección analizamos los resultados obtenidos.

En primer lugar mostramos en la Tabla 1 una clasificación de los estudios primarios obtenidos en base a las siguientes categorías: propuestas de ontologías de seguridad generales y centradas en un dominio concreto, trabajos teóricos y estudios centrados en la web semántica (tanto teóricos como propuestas específicas).

Categorías	Nº	Estudios
Ontologías de seguridad	3	[20], [21], [33]
Ontologías de domino	8	[1], [8], [11], [14], [15], [28], [34], [36]
Teóricos	4	[9], [10], [29], [27]
Seguridad en la Web Semántica	9	([4], [5], [19]), [23], [25], [26], [31], [32], [35]
Total	24	

Tabla 1: Clasificación de los estudios primarios

A continuación presentamos el marco de evaluación propuesto, el cuál es similar al utilizado en el trabajo [3] y pretende hacer una comparación y evaluación de estas ontologías desde varios puntos de vista distintos: una comparación general donde se realiza una medición de los elementos (conceptos, atributos, instancias, relaciones, etc) que contiene cada ontología, una comparación formal de las taxonomías utilizando para ello la metodología OntoClean [18] y por último se utiliza un subconjunto de las mediciones que se pueden realizar con OntoMetric [24].

Al intentar realizar la comparación formal de las ocho propuestas de ontologías de seguridad identificadas en la sección 4, nos encontramos con la problemática de que la mayoría o no están accesibles por web y que al intentar obtenerlas directamente por medio de los autores nos comunican que están aún en desarrollo. De todas formas aplicamos la comparación general y OntoMetric a las ontologías que tenemos, dejando como trabajo futuro la incorporación del resto de trabajos cuando estén disponibles.

5.1. Comparación general

En la Tabla 2 mostramos los resultados obtenidos en la medida de las propiedades generales de las ontologías.

	Kim [21]	Dobson [8]
Conceptos	73	87
Conceptos padre	20	15
Instancias	78	61
Media de profundidad de la herencia	2,06	2,84
Media del nº de conceptos relacionados	0,36	0,78
Media del nº de atributos por concepto	0,43	1,78
Media del nº de subclases	0,77	0,82
Nº de relaciones taxonómicas	53	72
Nº de relaciones no taxonómicas	11	24

Tabla 2: Comparación general

Podemos ver como ambas ontologías presentan algunas diferencias. Dobson utiliza un

árbol de herencia con mayor profundidad y los conceptos están más relacionados entre si y mejor definidos mediante un mayor uso de atributos.

5.2. OntoMetric

Este método se basa en la comparación de la importancia de los objetivos y las características de las ontologías para tratar de medir si pueden reutilizarse en nuevos proyectos. Este framework realiza una comparación de características agrupadas en 5 dimensiones: contenido representado, lenguaje, metodología y entorno software utilizado para construir la ontología, y además el coste de utilizarla en nuevos sistemas. Cada dimensión contiene un conjunto de factores que a su vez están compuestos por un conjunto de características que permiten su medición.

En nuestro marco de comparación vamos a utilizar principalmente la dimensión de contenido. Respecto a la dimensión lenguaje de representación, todas las ontologías que tratamos han sido implementadas mediante OWL.

Dentro de la dimensión de contenido nos encontramos con varias características descriptivas, a las cuales se les ha asignado una puntuación de 1 a 5 dependiendo de si el grado de cumplimiento es desde muy bajo hasta muy alto. Las características aparecen agrupadas por los siguientes factores: conceptos Tabla 3, relaciones Tabla 4, taxonomía Tabla 5 y axiomas Tabla 6.

Respecto al factor conceptos, Tabla 3, podemos observar como Kim describe de forma muy pobre los conceptos además de hacer muy poco uso de los atributos. De igual forma sucede en el factor relaciones, Tabla 4, en el que no describe de forma apropiada ni sus relaciones ni sus propiedades formales.

Factor Conceptos	**Kim [21]**	**Dobson [8]**
Conceptos esenciales	4	3
Conceptos esenciales en niveles superiores	5	5
Descripción correcta en lenguaje natural	1	3
La especificación formal coincide con el lenguaje natural	1	5
Los atributos describen los conceptos	1	4
Nº de conceptos	4	5

Tabla 3: Factor conceptos

Factor Relaciones	**Kim [21]**	**Dobson [8]**
Relaciones esenciales	4	4
Relacionan los conceptos adecuados	5	5
Descripción correcta en lenguaje natural	1	3
Aridad	2	3
Especificación de sus propiedades formales	1	4
Nº de relaciones	3	4

Tabla 4: Factor relaciones

En cuanto al factor taxonomía, Tabla 5, ambas ontologías carecen del uso de varias perspectivas para el mismo concepto, así como el uso de no_subclase_de y particiones exhaustivas. Por último, respecto al factor axiomas, Tabla 6, ambos hacen uso de axiomas aunque no definidos como conceptos independientes pero es en Dobson donde se hace un uso mayor y se les da una mayor utilidad tanto para inferencia como para verificar la consistencia.

Factor Taxonomía de Conceptos	**Kim [21]**	**Dobson [8]**
Varias perspectivas	1	1
Uso apropiado de no_subclase_de	1	1
Particiones exhaustivas apropiadas	1	1
Particiones disjuntas apropiadas	3	4
Profundidad máxima	2	3
Media de hijos por concepto	3	4

Tabla 5: Factor taxonomía de conceptos

Factor Axiomas	**Kim [21]**	**Dobson [8]**
Los axiomas responden consultas	2	4
Infieren conocimiento	2	4
Verifican la consistencia	3	5
Axiomas definidos como conceptos independientes	1	1
Nº de axiomas	2	4

Tabla 6: Factor axiomas

6. Conclusiones

Una de las primeras acciones que debe llevar a cabo una comunidad de investigadores en un determinado tema es elaborar, si no existe, una ontología que les permita compartir y consensuar

los conceptos básicos y sus relaciones. Esto en el campo de la seguridad aún no se ha conseguido. La mayoría de las propuestas están centradas en la web semántica o en dominios concretos y las referentes a ontologías de seguridad generales, representan la mayoría de los conceptos de seguridad presentes en la época en la que fueron creadas y trabajan bien sobre los escenarios para los que fueron concebidas, pero están lejos de ser ontologías de seguridad completas.

Del mismo modo, hemos podido comprobar como la mayoría de las ontologías de seguridad identificadas no están accesibles, siendo en muchos casos propuestas tempranas aún en fase de desarrollo, lo que requiere de un mayor esfuerzo por parte de la comunidad investigadora.

La definición de una ontología de seguridad completa es trabajo de la comunidad y no debe partir de cero, ya que la representación de todos los conceptos de seguridad sería inviable, sino partir de la unión de las propuestas definidas anteriormente. Por lo tanto, es necesario dotar a la comunidad de las metodologías y herramientas adecuadas que permitan actualizar la ontología reflejando la evolución y aparición de los nuevos conceptos de seguridad.

7. Agradecimientos

Este artículo es parte del proyecto ESFINGE (TIN2006-15175-C05-05), DEDALO (TIC2006-15175-C05-03) y RETISTRUST (TIN2006-26885-E) del Ministerio de Educación y Ciencia, y de los proyectos MISTICO (PBC-06-0082), DIMENSIONS (PBC-05-012-2) y DESERT (PBC-05-012-3) de la Consejería de Ciencia y Tecnología de la Junta de Comunidades de Castilla-La Mancha y el FEDER.

Referencias

[1] 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.

[2] Biolchini, J. y P. Gomes, Systematic Review in Software Engineering. 2005, Systems Engineering and Computer Science Department, UFRJ: Río de Janeiro, Brazil.

[3] Blomqvist, E., A. Öhgren, y 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.

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

[5] Denker, G., et al., Security for DAML Web Services: Annotation and Matchmaking, in The SemanticWeb - ISWC 2003. 2003, Springer Berlin / Heidelberg. p. 335-350.

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

[7] Dhillon, G. y J. Backhouse, Information system security management in the new millennium. Communications of the ACM, 2000. 43(7): p. 125-128.

[8] Dobson, G. y 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.

[9] DOD, Orange Book. Estándar DOD 5200.58-STD. 1970, Departamento de defensa de los EEUU.

[10] Donner, M., Toward a Security Ontology. IEEE Security and Privacy, 2003. 1(3).

[11] Fenz, S. y 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.

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

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

[14] Geneiatakis, D. y C. Lambrinoudakis, An ontology description for SIP security flaws. Computer Communications, 2006. In Press, Corrected Proof.

[15] Giorgini, P., H. Mouratidis, y N. Zannone, Modelling Security and Trust with Secure Tropos, in Integrating Security and Software Engineering: Advances and Future Visions. 2006, Idea Group Publishing.
[16] 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.
[17] Gruninger, M. y J. Lee, Ontology Applications and Design. Communications of the ACM, 2002. 45(2): p. 39-41.
[18] Guarino, N. y C. Welty, Evaluating ontological decisions with ONTOCLEAN. Communications of the ACM, 2002. 45(2): p. 61-65.
[19] Kagal, L. y T. Finin, Modeling conversation policies using permissions and obligations. AAMAS workshop on Agent communication, LNCS. Springer-Verlag, 2005.
[20] 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.
[21] Kim, A., J. Luo, y M. Kang. Security Ontology for Annotating Resources. in 4th International Conference on Ontologies, Databases, and Applications of Semantics (ODBASE'05). 2005. Agia Napa, Cyprus.
[22] Kitchenham, B., Procedures for performing systematic reviews (Joint Technical Report), in TR/SE-0401. 2004, Keele University, Sortware Engineering Group. Department of Computer Science. p. 33.
[23] Kwon, J. y 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] Lozano-Tello, A. y 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).
[25] Maamar, Z., N.C. Narendra, y 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, y 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. y P. Giorgini, An Introduction, in Integrating Security and Software Engineering: Advances and Future Visions. 2006, Idea Group Publishing.
[28] Mouratidis, H., P. Giorgini, y 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.
[29] 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.
[30] Ruíz, F., El Meta-Meta, las Ontologías y la Investigación en Ingeniería del Software. II Workshop en Métodos de Investigación y Fundamentos Filosóficos en Ingeniería del Software y Sistemas de Información, 2004.
[31] Tan, J.J. y S. Poslad, Dynamic security reconfiguration for the semantic web. Engineering Applications of Artificial Intelligence, 2004. 17(7): p. 783-797.
[32] Thuraisingham, B., Security standards for the semantic web. Computer Standards & Interfaces, 2005. 27(3): p. 257-268.
[33] Tsoumas, B. y 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.
[34] Undercoffer, J., A. Joshi, y J. Pinkston. Modeling Computer Attacks: An Ontology for Intrusion Detection. in The Sixth International Symposium on Recent Advances in Intrusion Detection. 2003: Springer.
[35] Vorobiev, A. y 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.
[36] Yu, E., L. Liu, y Mylopoulos, A Social Ontology for Integrating Security and Software Engineering, in Integrating Security and Software Engineering: Advances and Future Visions. 2006, Idea Group Publishing.