NIHIL INTENTATUM

Universidad Católica de Salta

Papeles De Mar Del Plata

Anales del IV Congreso Iberoamericano de Seguridad Informática

Papeles De Mar Del Plata

Anales del IV Congreso Iberoamericano de Seguridad Informática

NIHIL INTENTATUM

Universidad Católica de Salta

PAPELES DE MAR DEL PLATA

ANALES DEL IV CONGRESO IBEROAMERICANO DE SEGURIDAD INFORMÁTICA

COMPILADORES

Antonio Castro Lechtaler

Julio César Liporace

Jorge Ramió Aguirre

Universidad Católica de Salta

Salta

2007

Papeles de Mar del Plata: Actas del IV Congreso Iberoamericano de Seguridad Informática / Recopilado por Antonio Castro Lechtaler; Julio Cesar Liporace; Jorge Ramió Aguirre. - 1ª Ed. Salta: Universidad Católica de Salta - Eucasa, 2007.

606 p. ; 24 x 17 cm. (Anales Congreso)

ISBN 978-950-623-043-2

1. Seguridad Informática. I. Castro Lechtaler, Antonio, recop. II. Liporace, Julio Cesar, recop. III. Ramio Aguirre, Jorge, recop.

CDD 005.8

Campo Castañares, Salta, Provincia de Salta, (A4400EDD)
República Argentina
☎ + 54 - 387 – 426-8939 fax + 54 - 387 – 426-8800

ISBN: 978-950-623-043-2
Depósito legal: Argentina 2007

EDITOR: Sebastián Cañón, M.A.
PRODUCTOR: Cristian Cavaleiro
COMPOSICIÓN INTERIOR Y APOYO GRÁFICO: Señor Oscar Iturralde.

IMPRESO EN IMPRENTA DE DOCUPRINT S.A.
Rivadavia Nº 701, (C1002AAF).
Ciudad Autónoma de Buenos Aires, República Argentina.
☎ + 54 - 11 – 43 38 20 00 fax + 54 - 11 – 43 38 20 40

De esta edición se han impreso 300 ejemplares en el mes de noviembre de 2007.

PRINTED IN ARGENTINA - IMPRESO EN ARGENTINA

PAPELES DE MAR DEL PLATA

ANALES DEL IV CONGRESO IBEROAMERICANO DE SEGURIDAD INFORMÁTICA

COMPILADORES

Antonio Castro Lechtaler
Julio César Liporace
Jorge Ramió Aguirre

Universidad Católica de Salta
Salta
2007

COMITÉ DE HONOR

PRESIDENTE: Dr. Néstor AUZA

Presidente de la Comisión de Investigaciones Científicas de la Provincia de Buenos Aires
y Rector de la Universidad Nacional del Centro de la Provincia de Buenos Aires.

MIEMBROS

Ing. Héctor Carlos BROTTO
Rector de la Universidad Tecnológica Nacional

Ing. Norberto CAMINOA
Rector de la Universidad Nacional de Chilecito

Dr. Alfredo Gustavo PUIG
Rector de la Universidad Católica de Salta

General Ingeniero Guillermo SEVILLA
Presidente de CITEFA (Instituto de Investigaciones Científicas y Técnicas de las Fuerzas Armadas)

Dr. Manuel Aguirre TELLEZ
Decano de la Facultad de Ciencias Exactas
Universidad Nacional del Centro de la Provincia de Buenos Aires

Coronel Ingeniero Gustavo LANDA
Director - Decano de la Escuela Superior Técnica/Facultad de Ingeniería
Universidad del Ejército

Lic. Jorge Luis CAJAL
Miembro del Directorio
Comisión de Investigaciones Científicas de la Provincia de Buenos Aires

Arq. Luis De MARCO
Decano de la Facultad Regional Buenos Aires
Universidad Tecnológica Nacional

Ing. Claudio MONDADA
Decano Facultad de Ingeniería
Universidad Católica de Salta

Dr. Hugo Daniel SCOLNIK
Universidad de Buenos Aires

COMITÉ ORGANIZADOR

Ing. Antonio Ricardo Castro Lechtaler, MSc
Presidente

Dr. Jorge Ramió Aguirre,
Vicepresidente y Presidente del Comité de Programa

Lic. Julio César Liporace, EspCyS
Vicepresidente Ejecutivo

Dr. Nelson Acosta,
Vicepresidente Coordinador Local

DIRECTORES DE ÁREAS

Lic. Jorge Zaccagnini,
Director de Comunicación Social y Prensa

Mag. Lic. Carlos Alberto López,
Director de Relaciones Institucionales

Lic. Carlos Tomassino,
Director de Relaciones con las Universidades

Ing. Hugo Ballesteros,
Director de Relaciones con los Institutos de Investigación

DIRECTORES LOCALES

Lic. Oscar Noguez
Director en Buenos Aires

Ing. Roberto Giordano Lerena,
Director en Mar del Plata

Dr. Carlos García Garino
Director en Mendoza

Lic. Javier Díaz,
Director en La Plata

Mag. Ing. Beatriz Parra de Gallo,
Directora en Salta

Ing. Fernanda Carmona,
Directora en La Rioja

COMITÉ DE PROGRAMA

Presidente
Dr. Jorge Ramió Aguirre,
Universidad Politécnica de Madrid, España

MSc. Nicolás César Alfonso Antezana Abarca
Universidad Católica San Pablo, Perú

Dr. Javier Areitio Bertolín
Universidad de Deusto, España

Dr. Walter Baluja García
Instituto Superior Politécnico José Antonio Echeverría, Cuba

Dr. Joan Borrel Viader
Universidad Autónoma de Barcelona, España

Dra. Pino Caballero Gil
Universidad de La Laguna, España

Dr. Josep Domingo i Ferrer
Universidad Rovira i Virgili, España

Dr. Jeimy José Cano Martínez
Universidad de los Andes, Colombia

Dr. Adriano Mauro Cansian
Universidade Estadual Paulista, Brasil

Dr. Hugo César Coyote Estrada
Instituto Politécnico Nacional, México

Dr. Ricardo Dahab
Universidade Estadual de Campinas, Brasil

Dr. Enrique Daltabuit Godas
Universidad Nacional Autónoma de México, México

Dr. Jorge Dávila Muro
Universidad Politécnica de Madrid, España

Dr. Jorge Estrada Sarlabous
Academia de Ciencias de Cuba, Cuba

Dr. Jose Luís Ferrer-Gomila
Universidad de Las Islas Baleares, España

COMITÉ CIENTÍFICO

Dr. Juan Pedro Hecht
Universidad de Buenos Aires, Argentina

Dr. Carlos Marcelo Sánchez
Universidad de Buenos Aires, Argentina

WORKSHOP EN TÉCNICAS DE HACKING Y FORENSIA INFORMÁTICA

Fecha: martes 27 de noviembre de 2007
Seminario práctico de 4 horas

Parte 1 (2 horas)

"Técnicas de Inyección en Hacking de Aplicaciones Web"

Ponente: Chema Alonso
Ingeniero y Dr. en Informática, a falta de la lectura de tesis en este año 2007. Es Microsoft MVP Windows Security desde Julio de 2004. Consultor de Seguridad Informática durante los últimos años. Ha participado en las últimas 7 giras de seguridad de Microsoft y los Security Days. Participa activamente con los cuerpos de seguridad del estado y realiza en Informática 64 test de intrusión para grandes compañías. Ponente en decenas de conferencias de seguridad al año.

Temario:

- Introducción a las técnicas de inyección.
- SQL injection, XPath injection, LDAP injection, HTML injection
- Análisis de exploits - Explotación mediante técnicas a ciegas
- Herramientas y caso práctico

Parte 2 (2 horas)

"Utilización de Patrones de Comportamiento en el Análisis Forense Informático"

Ponente: D. Julio César Ardita
Licenciado en Sistemas y Master en Gestión de las Telecomunicaciones. Es fundador del CISIar, Centro de Investigación en Seguridad Informática Argentina. Consultor de Seguridad Informática, es ponente invitado en decenas de congresos nacionales e internacionales. Desde Cybsec Security Systems S.A. es director de proyectos de investigación sobre sistemas de detección de intrusiones y penetration test, así como profesor en decenas de cursos de seguridad en Latinoamérica.

Temario:

- Características de los incidentes de seguridad internos
- Análisis forense informático
- Metodología de análisis de patrones de comportamiento del intruso
- Aplicación real y resultados obtenidos

PROGRAMA GENERAL ACADÉMICO

Lunes 26 de Noviembre (Sesiones Plenarias)	
10 hs - 11 hs	**11 hs - 12 hs**
Atacando RSA mediante un nuevo método de factorización de enteros	Seguridad y composición de protocolos criptográficos
Dr. Hugo Scolnik: Universidad de Buenos Aires, Argentina	**Dr. Alejandro Hevia; Universidad de Chile, Chile**

Martes 27 de Noviembre (Sesión Plenaria)
12:15 hs a 13:15 hs
Criptografía post-cuántica **Dr. Paulo Barreto; Universidad de Sao Paulo, Brasil**

Martes 27 de Noviembre (09:00 hs a 11:00 hs y 11:15 hs a 12:15 hs)	
Sala 1 (SESIÓN MM1)	**Sala 2 (SESIÓN MM2)**
Construcción de funciones Bent de n + 2 variables a partir de las funciones duales de funciones Bent de n variables. **Joan-Josep Climent, Francisco J. García, Verónica Requena (España)**	Medidas de Seguridad para ficheros no informatizados. **Javier Sempere Samaniego (España)**
Representation of Boolean maps through Hamiltonian paths. **Morales Luna, Rosaura Palma Orozco (México)**	Auditorias de Seguridad en Protección de Datos. **Ángel Igualada Menor (España)**
Performance Evaluation of Cryptographic Algorithms in JCOP41 Smart Card. **Matheus F. Oliveira, Marco A. A. Henriques (Brasil)**	Desarrollo y Mantenimiento Seguro de Software para Pymes: Moprosoft alineado a ISO/IEC 17799:2005. **Nancy Velásquez (Ecuador)**
Prediciendo secuencias producidas por un generador congruente lineal sobre curvas elípticas. **Jaime Gutiérrez, Álvar Ibeas (España)**	Hacia un Proceso sistemático para el desarrollo de sistemas Grid Seguros con Dispositivos Móviles **David G. Rosado, Javier López, Eduardo Fernández-Medina, Mario Piattini (España)**
Criptoanálisis del generador shrinking: una nueva propuesta basada en un time-memory trade-off. **M. E. Pazo-Robles, Amparo Fúster Sabater (Argentina)**	Construcción de un CMI de la Seguridad: Selección de indicadores mediante un sistema experto probabilística. **Daniel Villafranca, Luis Enrique Sánchez, Eduardo Fernández-Medina, Mario Piattini (España)**
StegSecret: una herramienta pública de estegoanálisis. **Alfonso Muñoz Muñoz, Justo Carracedo Gallardo (España)**	Concepción, Diseño e Implantación de un Laboratorio de Seguridad Informática **María Eugenia Corti, Marcelo Rodríguez, Gustavo Betarte (Uruguay)**

Martes 27 de Noviembre (14:30 hs a 16:30 hs y 16:45 hs a 17:45 hs)	
Sala 1 (SESIÓN MT1)	**Sala 2 (SESIÓN MT2)**
Autómatas celulares caóticos en la generación de funciones hash resistentes a los ataques de colisiones diferenciales. **Juan Pedro Hecht (Argentina)**	Buenas prácticas de elicitación de los requerimientos de seguridad. **Susana C. Romaniz (Argentina)**
A Signature Scheme based on Asymmetric Bilinear Pairing Functions. **Routo Terada, Denise H. Goya (Brasil)**	Evaluación de Riesgo en las Tecnologías de Información y Comunicaciones orientada a Organismos Públicos. **Pablo Andrés Pessolani (Argentina)**
A Class of Secret Sharing Schemes. **J.C. Ku, Horacio Tapia-Recillas (México)**	AUDISEG: Una metodología para la auditoría de la seguridad física del ambiente informático en el sector comercial. **Sandra Cristina Riascos, Juan Carlos Guerrero, Luís Byron Calvache, Jesús Eduardo Campaña (Colombia)**
Esquemas de reparto de secretos en términos de códigos producto. **Policarpo Abascal, Juan Tena (España)**	La Universidad Simón Bolivar a la luz de los controles de seguridad de las ISO - 17799/27001. **Vidalina De Freitas (Venezuela)**
Evitando el Replay attack en Protocolos de Intercambio Equitativo con Requisitos de Privacidad. **M. Magdalena Payeras-Capellà, Macià Mut-Puigserver, Llorenç Huguet-Rotger, Josep Lluís Ferrer-Gomila (España)**	Revisión sistemática y comparación de ontologías en el marco de la seguridad. **Carlos Blanco, Joaquín Lasheras, Rafael Valencia-García, Eduardo Fernández-Medina, Ambrosio Toval, Mario Piattini (España)**
Vulnerabilidad a un Ataque de Repetición en un Protocolo de Seguridad. **Macià Mut-Puigserver, Josep Lluís Ferrer-Gomila, Magdalena Payeras-Capellà, Llorenç Huguet-Rotger (España)**	

Miércoles 28 de Noviembre (09:00 hs a 11:00 hs y 11:15 hs a 13:15 hs)	
Sala 1 (SESIÓN XM1)	**Sala 2 (SESIÓN XM2)**
Análisis de las medidas de distancia entre sesiones para la clasificación de intrusos. **Sebastián García (Argentina)**	Análisis de la Seguridad en Ecosistemas de Ambiente Inteligente. **Juan J. Ortega, Antonio Maña, Antonio Muñoz, Alejandro Gómez(España)**
NCD Based Masquerader Detection Using Enriched Command Lines. **Maximiliano Bertacchini, Carlos E. Benitez (Argentina)**	Nuevas Tendencia en Fraude electrónico. Relación entre malware y criptografía. **Delgado, José María Cámara (España)**
Metodología para la Evaluación de la Seguridad de Aplicaciones Web frente a Ataques Blind SQL Injection. **Chema Alonso, Rodolfo Bordón, Marta Beltrán, Antonio Guzmán (España)**	Sistema de identificación biométrica mediante patrón de iris utilizando operadores morfológicos y representación multiescala. **Alberto de Santos Sierra, Carmen Sánchez Ávila, Raúl Sánchez Reíllo (España)**
w3af – Web Application Attack and Audit Framework. **Andrés Riancho (Argentina)**	Attacking the Giants: Exploiting SAP Internals. **Mariano Nuñez Di Croce (Argentina)**
Transacciones Seguras para Sistemas Móviles por medio de Relaciones de Confianza. **Chadwick Carreto Arellano, Rolando Menchaca Garcia, Rolando Menchaca Méndez (México)**	Implementación de una Interfaz de Administración para Java Cards. **Luis Adrián Lizama Pérez, Roberto León Oramas, Tirso Alejandro (México)**
Técnicas antiforenses: Ocultando información en HFS+. **Carlos Enrique Nieto Lara (Colombia)**	Message-embedding from a control-theoretical point of view. **Gilles Millérioux, José María Amigó, Jamal Daafouz (España)**
Servicio de No Repudio para Marketing y Comercio basados en Servicios de Localización. **Benjamín Ramos, Ana I. González-Tablas, Arturo Ribagorda, Daniel Garzón (España)**	

Miércoles 28 de Noviembre (14:30 hs a 16:30 hs)	
Sala 1 (SESIÓN XT1)	**Sala 2 (SESIÓN XT2)**
Analysis of security protocol MiniSec for Wireless Sensor Networks. **Llanos Tobarra, Diego Cazorla, Fernando Cuartero (España)**	Arquitectura Estándar para Identificación Digital. **Chadwick Carreto Arellano, Rolando Menchaca García, Jesús Martínez Castro (México)**
Análisis Forense de Equipos de Telefonía Celular. **Rubén Vázquez-Medina, Lucio Santes-Galván, Alberto Ramos Toxtle (México)**	Performance issues to consider when applying Digital Signature in XML documents. **Eduardo Esteban Casanovas, Marcelo da Cruz Pinto (Argentina)**
SCMM-TOOL: Desarrollando una herramienta para gestionar la seguridad de los sistemas de información en las PYMES basada en Esquemas predefinidos **Luís Enrique Sánchez, Daniel Villafranca, Antonio Santos-Olmo, Eduardo Fernández-Medina, Mario Piattini (España)**	VALI - Herramienta de correlación de mensajes de bitácoras basada en relojes vectoriales. **Roberto Gómez, Julio César Rojas, Erika Mata (México)**
OTPM: Utilización del teléfono móvil como token de autenticación en servicios de banca electrónica. **Jorge Munilla, Alberto Peinado, Bernardo Quintero, Javier Téllez (España)**	Una propuesta de Autenticación Unificada Basada en la Sincronización de LDAP con Microsoft Active Directory. **Federico Herman Lutz, Sebastián Azubel (Argentina)**

Señores Congresales del IV Congreso Iberoamericano de Seguridad Informática.

Para la Universidad Católica de Salta es un gran honor haber sido invitada a publicar, a través de su fondo editorial, estos Papeles de Mar del Plata – Actas del IV Congreso Iberoamericano de Seguridad Informática, resultado del Congreso Internacional que se realizará del 25 al 28 de noviembre de 2007 en nuestro país con ese nombre.

Los 48 trabajos que aquí se presentan, aprobados por un Comité de Expertos Internacional de muy alto nivel profesional que hoy se ponen a consideración de la comunidad de investigadores de Iberoamérica y del mundo entero, representan una importante contribución al desarrollo de la criptografía y la seguridad informática. Estamos por ello seguros, que serán sin duda de gran valor para aquellos que trabaja en estas temáticas.

Nuestra Universidad, a través de su Facultad de Ingeniería, ha dado una importante prioridad a la enseñanza e investigación en las áreas de la informática y las telecomunicaciones, carreras que se dictan en ella al más alto nivel, con destacados profesionales que participarán de este significativo evento.

Deseamos entonces, darles la bienvenida a las personalidades extranjeras que hoy nos visitan, como así también a los numerosos colegas de nuestro país. A todos ellos, nuestros más afectuosos saludos. Son bienvenidos en nuestra patria.

Salta, noviembre de 2007

Dr. ALFREDO GUSTAVO PUIG
Rector
Universidad Católica de Salta

PROLOGO DE LA COMISIÓN ORGANIZADORA

Estimados Colegas,

A fines del año 2006, cuando Jorge Ramió Aguirre concurría a dictar un curso de postgrado en la Especialización en Criptografía y Seguridad Teleinformática que se dicta todos los años en la Escuela Superior Técnica de la Universidad del Ejercito desde el año 2002, nos convocó y entusiasmó a los que en la República Argentina estamos de alguna manera vinculados a la Criptografía y a la Seguridad a organizar el IV Congreso Iberoamericano que se viene haciendo con singular éxito.

A partir de allí, hemos tratado de ir armando el Congreso del que a partir de hoy ustedes podrán participar en esta ciudad de Mar del Plata. Esperamos que ella, les resulte grata y acogedora.

Como ocurre en estos casos, no han sido pocos los problemas que hemos debido ir superando para llegar a esta fecha. Y son varias las Instituciones a las que les debemos nuestro agradeciendo por su colaboración recibida desde el primer momento que les planteamos la realización de este evento.

En primer lugar, a la Comisión de Investigaciones Cientificas de la Provincia de Buenos Aires como Institución, y en particular a su Presidente y Rector de la Universidad Nacional del Centro de la Provincia de Buenos Aires Dr. Néstor Auza quien fue el primero en brindarnos su sincero apoyo. También a todos aquellos que forman parte de la Comisión de Honor, que de alguna manera han colaborado a que este Congreso esté siendo inaugurado, en particular a las autoridades nacionales y universitarias a las que estamos muy agradecidos.

En ésta como en toda reunión científica, sus objetivos se enfocan para observar hacia donde se dirige el estado del arte de la actividad en particular, y para convocar a los expertos a un intercambio de reflexiones que permitan avizorar -en singular oportunidad- los nuevos desafíos.

No dudamos que el primero se ha cumplido. El numeroso conjunto de ponencias aprobadas con referato internacional así lo prueba. El segundo seguramente será también una realidad porque esta disciplina ya dejó de ser parte de otras disciplinas, para ocupar un lugar propio manejado por verdaderos profesionales en las temáticas.

Esperemos que estos Papeles de Mar del Plata sean una guia para aquellos que trabajan e investigan en estas ciencias con el objeto de correr cada día más las fronteras del conocimiento.

Mar del Plata, noviembre de 2007

Lic. JULIO CÉSAR LIPORACE, EspCySeg.
Vicepresidente Ejecutivo
Comité Organizador
IV Congreso Iberoamericano de Seguridad Informática

Prof. Ing. ANTONIO CASTRO LECHTALER, MSc
Presidente
Comité Organizador
IV Congreso Iberoamericano de Seguridad Informática

PRÓLOGO DEL COORDINADOR DE LA RED TEMÁTICA CRIPTORED

Estimados compañeros:

Por cuarta vez nos juntamos como cada dos años en este espacio académico y de investigación propuesto por la Red Temática CriptoRed, y que hemos denominado Congreso Iberoamericano de Seguridad Informática CIBSI, para hacer un repaso del estado del arte en las materias propias de la seguridad de la información, evento que dentro de Iberoamérica congrega al mayor número de representantes y expertos en seguridad informática de los países que la conforman: Latinoamérica, Portugal y España.

CIBSI 2007 cuenta con la especial acogida de la Universidad del Centro de la Provincia de Buenos Aires, quien organiza este congreso conjuntamente con la Universidad Politécnica de Madrid, a cuyos directivos así como a todos y cada uno de los miembros del Comité Organizador deseo agradecer desde estas páginas su buen hacer y la excelente hospitalidad que nos brindan a todos los asistentes.

De 69 trabajos recibidos, un selecto grupo de 43 expertos de 13 países (Argentina, Brasil, Chile, Colombia, Cuba, Ecuador, España, México, Panamá, Perú, Portugal, Venezuela y Uruguay) ha seleccionado 48 documentos, de los que al final se presentan en este evento 43, y que proceden de investigadores de Argentina, Brasil, Colombia, Ecuador, España, México, Uruguay y Venezuela.

Así mismo, el congreso cuenta con tres conferenciantes invitados a sesiones plenarias, el Dr. Paulo Barreto de Brasil, el Dr. Alejandro Hevia de Chile y el Dr. Hugo Scolnik de Argentina, y se impartirá de forma simultánea un Workshop sobre Técnicas de Hacking y Forensia Informática, a cargo de los expertos D. Julio César Ardita de Argentina y D. José María Alonso de España.

Ya van quedando para el histórico aquellos gratos recuerdos de las ediciones de Morelia en 2002 y en el DF en 2003, ambos en México, así como el de Valparaíso en Chile en 2005, observando que en cada edición aumenta la cantidad de los trabajos presentados, participan más países y más grupos de investigación, lo que permite augurar excelentes expectativas de crecimiento para las futuras ediciones de CIBSI en el año 2009 y siguientes.

Como coordinador de CriptoRed, comunidad virtual de expertos en seguridad de la información con más de 650 miembros de 185 universidades y 240 empresas, que son el verdadero motor de este congreso, sólo puedo reiterar mis agradecimientos a todos, organizadores, autores, revisores, patrocinadores y asistentes, por permitir que este gran esfuerzo que todos hemos realizado se convierta nuevamente en una realidad, esta vez ante el marco excepcional de la hermosa ciudad de Mar del Plata y en un bello país de paisajes y gentes, Argentina.

A todos, un caluroso abrazo con todo mi afecto.

Mar del Plata, noviembre de 2007

Dr. JORGE RAMIÓ AGUIRRE
Coordinador de CriptoRed

Presidente
Comité de Programa
IV Congreso Iberoamericano de Seguridad Informática

INDICE

Revisión sistemática y comparación de ontologías en el marco de la seguridad

Carlos Blanco[1], Joaquín Lasheras[2], Rafael Valencia-García[2], Eduardo Fernández-Medina[1], Ambrosio Toval[1], 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, España. FAX: +34 926 295354. Teléfonos: +34 926 295300 ext. 3747, 3744, 3715. {Carlos.Blanco, Eduardo.FdezMedina, Mario.Piattini}@uclm.es

[2] Dept. de Informática y Sistemas. Facultad de Informática. Universidad de Murcia. Campus Universitario de Espinardo. 30011 Murcia, España. FAX: +34 968 364151. Teléfonos: +34 968 398556, +34 968 398522, +34 968 364603. {jolave, valencia, atoval}@um.es

Abstract. Las ontologías soportan formalmente los conceptos y relaciones que se manejan en cualquier comunidad científica, proporcinando una mejor comunicación y reutilización. La seguridad de la información es un campo de vital importancia en el que se está aplicando este enfoque, de modo que existen varias propuestas que deben ser analizadas. En este trabajo realizamos un estudio en profundidad del estado del arte mediante la técnica de revisión sistemática, localizando, analizando y comparando mediante un marco formal las principales propuestas de ontologías de seguridad. Concluimos el trabajo reflexionando sobre el estado prematuro de las propuestas existentes y la necesidad de un mayor esfuerzo por parte de la comunidad investigadora.

Keywords: revisión sistemática, comparativa, ontología, seguridad.

1 Introducción

La seguridad de la información es un aspecto crucial y necesario en los sistemas de información (SI) que debido a su importancia no debe ser considerada de forma aislada, sino como un elemento presente en todas las etapas del proceso de desarrollo [1-3]. De esta forma, la confidencialidad, seguridad y privacidad de la información han pasado a ser aspectos críticos y de vital importancia para la sociedad [4], llegando algunos autores a señalar que la supervivencia de las organizaciones depende de la correcta gestión de la seguridad y confidencialidad de la información [5].

Por otro lado, las ontologías nos permiten especificar explícitamente una conceptualización [6], es decir, son una representación formal y estructurada del conocimiento que nos proporciona una mejor comunicación, reutilización y organización del conocimiento e inferencia computacional [7-9]. De este modo, el

principal objetivo de las ontologías es el establecimiento de acuerdos ontológicos que disminuyan la ambigüedad del lenguaje y sirvan como base para la comunicación entre agentes y el filtrado de conocimiento en base a metamodelos [10].

Dada la importancia de la seguridad y los beneficios obtenidos por el uso de ontologías, la definición de una ontología que les permita compartir y consensuar los conceptos y relaciones de los términos que manejan ha sido identificada como una área de investigación importante y un reto dentro de la comunidad de la ingeniería de seguridad [3, 11, 12].

En este artículo hacemos un estudio de las propuestas existentes de ontologías en el marco de los desarrollos de seguridad utilizando un protocolo formal [13] para aplicar la técnica de revisión sistemática [14]. Mediante esta técnica podemos identificar, evaluar e interpretar todos los estudios importantes o significativos, llamados estudios primarios, para una pregunta de investigación en particular. La revisión sistemática consta principalmente de una etapa de planificación en la que se identifican los objetivos y restricciones y otra de desarrollo en la que se extraen los estudios primarios y su información relevante.

Finalmente se realiza una comparación formal entre las ontologías identificadas dentro de estos estudios primarios. La comparación se basa en el trabajo presentado en [15] que nos permitirá extraer conclusiones sobre lo bien construidas que están dichas ontologías.

El resto de este artículo está organizado de la siguiente forma: en primer lugar realizamos la planificación de la revisión sistemática en las secciones 2 y 3, para posteriormente en la sección 4 ejecutar la revisión y obtener los estudios primarios. Las principales propuestas de ontologías de seguridad se analizan en la sección 5 y se comparan mediante un marco formal en la sección 6, finalizando con las conclusiones en la sección 7.

2 Formalización de la pregunta

En este apartado, siguiendo el protocolo de revisión sistemática, se muestra como la planificación de la revisión comienza definiendo de forma clara los objetivos.

2.1 Foco de la pregunta

El primer paso es definir el *foco de la pregunta*, en nuestro caso la localización de trabajos que realicen aportaciones importantes sobre el desarrollo de ontologías centradas en aspectos de seguridad.

2.2 Amplitud y calidad de la pregunta

Para definir la amplitud y calidad de la pregunta, nos basamos en la respuesta a una serie de apartados en los que se analiza el problema a tratar, se propone la pregunta de investigación y el conjunto de palabras clave identificadas, así como los resultados que esperamos obtener y cómo serán analizados.

En la introducción se destacan la importancia de la seguridad como aspecto relevante para todas las etapas del proceso de desarrollo, así como los beneficios obtenidos por la utilización de ontologías, principalmente por la unificación y compartición de conocimiento en una determinada comunidad. Por ello, y vista la necesidad de definir una ontología de seguridad identificada por varios autores, definimos nuestro *problema* como la búsqueda de trabajos relevantes dentro de la ingeniería ontológica aplicados en el campo de la seguridad de la información.

Una vez conocido el problema, podemos definir la *pregunta de investigación* de esta revisión como ¿qué trabajos aplicados a la seguridad se han llevado a cabo dentro de la ingeniería ontológica? Posteriormente, definimos el conjunto de *palabras clave* y conceptos relacionados que aparecen en la Tabla 1, los cuales sirven como base para la creación de las consultas a realizar.

Tabla 1. Palabras clave y conceptos relacionados.

Área	**Palabras clave**	**Conceptos relacionados**
Ontologías	Ontology	Ontological engineering
	OWL	
	RDF	
	DAML	
Seguridad	Security	Secure
	Privacy	

La revisión no parte de ningún grupo de trabajos primarios iniciales, de modo que todos los trabajos incluidos serán derivados de la aplicación y cumplimiento de los criterios definidos. Siendo la *población* a analizar el conjunto de trabajos presentes en las fuentes seleccionadas (ver sección 3.1) y el idioma de estudio el inglés.

Como *resultado* detectamos las propuestas relevantes en cuanto al uso de ontologías dentro del marco de la seguridad, siendo la *medida de salida* la clasificación de los estudios por el área en la que se centran y la comparación de las principales propuestas mediante un marco formal de comparación de ontologías. Por lo tanto, los beneficiarios de este trabajo serán las personas (académicos, investigadores, profesionales, etc) relacionadas directamente con la ingeniería ontológica aplicada a la seguridad interesadas en conocer trabajos actuales en ambos campos o de forma independiente en alguno de ellos.

3 Método de revisión

En esta sección, siguiendo el protocolo de la revisión sistemática, se define la estrategia de búsqueda, centrándonos en la selección de fuentes de búsqueda, del procedimiento y criterios a seguir para la selección de los estudios primarios y en la ejecución de la revisión planificada.

3.1 Selección de fuentes

El criterio para la selección de las fuentes de búsqueda se basa en la recomendación de expertos[1] en las áreas tanto de la ingeniería ontológica como de la seguridad, los cuales según su experiencia profesional han considerado las siguientes *fuentes*: ACM Digital Library, IEEE Digital Library, Science Direct, Schoolar Google y DBLP. Todas ellas ofrecen artículos de calidad sobre el área de estudio, son accesibles vía web y presentan motores de búsqueda. Además, para asegurar que el trabajo sea lo más completo posible, tras la ejecución de la revisión sobre dichas fuentes se realiza una fase de refinado en la que se incluyen estudios importantes que no han sido obtenidos de dichas fuentes.

3.2 Selección de estudios

Una vez seleccionadas las fuentes, se define el procedimiento de selección de estudios que incluye los criterios de inclusión y exclusión. El *procedimiento* de selección de estudios primarios es un proceso iterativo e incremental a ejecutar en cada fuente seleccionada y consiste en adecuar la cadena de búsqueda al motor de la fuente para, a continuación, ejecutar la consulta y obtener un conjunto de estudios que son filtrados. En primer lugar se utiliza el criterio de inclusión para reducir el conjunto y quedárnos con los estudios relevantes. A este conjunto se le aplicará el criterio de exclusión para obtener los estudios primarios.

Mediante el *criterio de inclusión* realizamos un análisis sobre el *título*, *palabras clave* y *abstract* de cada documento obtenido, para descartar en una primera instancia el mayor número de trabajos que no realicen contribuciones sobre la seguridad dentro de la ingeniería ontológica. Posteriormente, mediante el *criterio de exclusión*, nos centramos principalmente en el *abstract* y *conclusiones*, entrando en más detalle en los trabajos que lo requieran, para así obtener los estudios primarios que realizan aportaciones significativas en el campo de estudio.

3.3 Ejecución de la selección

En esta sección se enumeran los estudios primarios obtenidos tras la ejecución de la revisión sistemática -un total de 28- sobre la lista de fuentes seleccionadas y su posterior fase de refinamiento.

- Amaral et al. "An Ontology-based Approach to the Formalization of Information Security Policies" [16].
- Denker et al. "Security for DAML Web Services: Annotation and Matchmaking" [17].
- Denker et al. "Security in the Semantic Web using OWL" [4].
- Departamento de defensa de los EEUU. "Orange Book" [18].

[1] De aquí en adelante, cuando nos refiramos al grupo de expertos, consideraremos dicho grupo como el formado por los autores de este trabajo.

- Dobson et al. "Revisiting Ontology-Based Requirements Engineering in the age of the Semantic Web" [9].
- Donner. "Toward a Security Ontology" [11].
- Fenz et al. "Ontology based IT-security planning" [19].
- Firesmith. "A Taxonomy of safety-related requirements" [20].
- Geneiatakis et al. "An ontology description for SIP security flaws" [21].
- Giorgini et al. "Modelling Security and Trust with Secure Tropos" [22].
- Kagal et al. "Modeling conversation policies using permissions and obligations" [23].
- Karyda et al. "An ontology for secure e-government applications" [24].
- Kim et al. "Security Ontology for Annotating Resources" [25].
- Kwon et al. "Visual modelling and formal specification of constraints of RBAC using semantic web technology" [26].
- Lee et al. "Building Problem Domain Ontology from Security Requirements in Regulatory Documents" [27].
- Maamar et al. "Towards an ontology-based approach for specifying and securing Web services" [28].
- McGibney et al. "A service-centric model for intrusion detection in next-generation networks" [29].
- Mouratidis et al. "An Ontology for Modelling Security: The Tropos Approach" [30].
- Mouratidis et al. "Integrating Security and Software Engineering: An Introduction" [3].
- Raskin et al. "Ontology in information security: a useful theoretical foundation" [31].
- Tan et al. "Dynamic security reconfiguration for the semantic web" [32].
- Thuraisingham. "Security standards for the semantic web" [33].
- Tsoumas et al. "Towards an Ontology-based Security Management" [12].
- Undercoffer et al. "Modeling Computer Attacks: An Ontology for Intrusion Detection" [34].
- Vorobiev et al. "Security Attack Ontology for Web Services" [35].
- Yu et al. "A Social Ontology for Integrating Security and Software Engineering" [36].
- Zhou et al. "An Integrated QoS-Aware Service Development and Management Framework" [37].
- Zhou et al. "Ontology Based Software Reliability Modelling" [38].

4 Extracción de información

Una vez identificados los estudios primarios se extrae su información relevante. Para ello se define un *formulario* en el que almacenar la información extraída y un *criterio de inclusión y exclusión de información*, basado en la adecuación con los objetivos, identificando el área en el que cada trabajo se centra, así como las aportaciones de interés que realiza.

De este modo, el formulario se estructura en varias partes: una de datos generales en la que aparecen el título, publicación, autores y referencia en formato EndNote, seguida de una descripción general en la que se identifica el área del estudio y se realiza un pequeño resumen, para concluir con un apartado de aspectos a destacar, en el que se incluyen comentarios y figuras relevantes.

Posteriormente en la sección de resultados, Tabla 2, podemos ver un resumen de cómo se han clasificado todos los estudios primarios identificados en base a las áreas: ontologías de seguridad (tanto generales como aplicadas a un dominio concreto) trabajos teóricos que refuerzan la importancia de las ontologías de seguridad y trabajos teóricos y prácticos referidos a la web semántica.

En el resto de esta sección analizamos cada estudio primario realizando un resumen de la información extraída. Por restricciones de espacio nos centraremos sólo en aquellos trabajos que realizan propuestas de ontologías de seguridad que posteriormente compararemos.

4.1 Denker et al. "Security in the Semantic Web using OWL" [4] y "Security for DAML Web Services: Annotation and Matchmaking" [17].

En estos trabajos se desarrolla una ontología enfocada a la creación de anotaciones seguras para los servicios web, cuyo objetivo es representar conceptos de seguridad bien conocidos y proporcionar notaciones que nos permitan la interconexión entre varios estándares de seguridad.

La ontología está formada principalmente por dos subontologías: "security mechanisms" – más general - y otra denominada "credential" –esta última centrada en mecanismos de autentificación, y fue desarrollada en primer lugar en DAML en [17] y posteriormente en OWL en [4].

4.2 Dobson et al. "Revisiting Ontology-Based Requirements Engineering in the age of the Semantic Web" [9].

Considerando el auge de la Web semántica realizan un estudio sobre el panorama de la ingeniería de requisitos enfocada desde el punto de vista ontológico y proponen una "dependability ontology" en OWL que incluye aspectos de seguridad tales como "dependability", "reliability", "availability", "integrity", "confidentiality" o "safety".

4.3 Fenz et al. "Ontology based IT-security planning" [19].

Se centran en la seguridad de pequeñas y medianas empresas, proponiendo una solución integral de seguridad en TI que incluye análisis de riesgos de bajo coste y análisis de amenazas.

La ontología está compuesta por varias subontologías, siendo su parte central la subontolología "threat" que trata directamente las amenazas incluyendo contramedidas, infraestructuras amenazadas y métodos de evaluación. Las demás subontologías son: "attribute" con los conceptos para modelar el impacto de las

amenazas, "infraestructure" que describe las infraestructuras, "role" para representar la jerarquía de la empresa y "person" para modelar aspectos de seguridad asociados a personas relevantes para el modelado de la seguridad de forma que cada persona tiene n roles.

4.4 Firesmith "A Taxonomy of safety-related requirements" [20].

En el trabajo se identifica como objetivo principal de un ingeniero de *safety* el identificar los requisitos para proteger activos valiosos como el personal, la propiedad o el entorno frente a la ocurrencia de amenazas poco frecuentes. A esta crítica tarea no se le suele prestar atención en la fase de especificación de requisitos, dificultando asegurar que las arquitecturas incorporan las salvaguardas adecuadas. Para ello proponen una taxonomía de requisitos *safety* dividida en 4 categorías: *requisitos safety*, derivados del análisis de amenazas para los activos del sistema; *requisitos con significado safety*, cualquier otro tipo de requisito (funcional, no funcional) que cumplen una misión primaria del sistema, sin ser safety, pero que causan amenazas o incidentes safety; *safety constraints*, derivados de leyes, normas, estándares y las mejores prácticas industriales; y por último, *safety system requirements* derivados de los objetivos de negocio del sistema. En el trabajo se destaca que estos requisitos tienen características reutilizables, para lo cual una ontología se presenta como elemento básico.

4.5 Karyda et al. "An ontology for secure e-government applications" [24].

Crean una ontología de seguridad con el fin de capturar el conocimiento de los expertos y ser usada por los desarrolladores para incluir requisitos de seguridad y para la toma de decisiones.

Aplican dicha ontología en dos escenarios del área de e-goverment, validándola mediante consultas nRQL: un sistema e-tax utilizado para los ciudadanos para realizar operaciones como el pago de tasas y un sistema de voto e-voting.

4.6 Kim et al. "Security Ontology for Annotating Resources" [25].

Los autores utilizan OWL para desarrollar, en base a siete subontologías, una ontología de seguridad enfocada a la representación de aspectos funcionales de recursos que presente una jerarquía de clases fácil de usar y de extender.

La ontología nos permite describir información de seguridad como mecanismos, protocolos, algoritmos y credenciales, en varios niveles de detalle, siendo capaz de representar la mayoría de aspectos de seguridad sobre cualquier recurso electrónico.

Profundizando en su arquitectura podemos ver como tres subontologías están basadas en ontologías existentes en DAML: "service security" para anotar de forma segura servicios web, "agent security" para consultar información de seguridad asociada a los recursos e "information object" para describir la seguridad asociada a los parámetros de servicios web. Por otro lado tenemos las cuatro ontologías

restantes: "main security" encargada de describir protocolos, mecanismos o políticas de seguridad, "credentials" para especificar mecanismos de autenticación, "security algorithms" que describe varios algoritmos de seguridad y "security assurance" que identifica distintos estándares que garantizan la seguridad.

4.7 Lee et al. "Building Problem Domain Ontology from Security Requirements in Regulatory Documents" [27].

Se pretende identificar requisitos de seguridad para certificación y acreditación, los cuales están expresados en documentos de normas y que por su naturaleza no-funcional implica complejas restricciones en el comportamiento de los sistemas software, siendo difíciles de controlar, entender y predecir. Para ello presentan un marco de trabajo que integra técnicas de ingeniería del software y del conocimiento. En concreto se propone el uso de un lenguaje común a través de una metodología para extraer conceptos expresados en base a documentos, en este caso documentos de normas utilizados por el DITSCAP - *Department of Defense Information Technology Security Certification and Accreditation Process*. Este lenguaje común establece lo que ellos denominan una ontología del dominio del problema (PDO).

4.8 Mouratidis et al. "An Ontology for Modelling Security: The Tropos Approach" [30] y "Modelling Security and Trust with Secure Tropos" [22].

La metodología Tropos[2] considera dos enfoques en el desarrollo software: un proceso orientado a la seguridad y otro a la gestión de la confiabilidad de los resultados. Dicha metodología está inspirada en estructuras sociales y organizacionales y adapta componentes del marco de modelado i* para el cuál se ha descrito una ontología social [36].

Los autores, con la intención de poder soportar aspectos de seguridad, extienden los conceptos principales de i* (actores, objetivos, tareas, recursos y dependencias) con nuevos conceptos de seguridad: restricciones de seguridad, entidades seguras (objetivos, tareas y recursos seguros) y dependencias seguras entre actores. Para soportar estos nuevos conceptos también extienden tanto la parte gráfica como la gramática del modelo.

4.9 Tsoumas et al. "Towards an Ontology-based Security Management" [12].

Basándose en la definición de una ontología de seguridad crean un marco que permite la adquisición y gestión del conocimiento referente a la seguridad en SI. Para poder almacenar la información relacionada con la seguridad y compartir y reutilizar la ontología de seguridad definida en OWL, extienden el extándar DMTF Common Information Model (CIM) enriqueciéndolo con semántica ontológica.

[2] http://www.troposproject.org

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

Desarrollan una ontología en DAML+OIL y DAMLJessKB para la lógica de la ontología que les permite especificar los modelos de ataque a computadores tras haber analizado unas 4000 vulnerabilidades y las estrategias correspondientes que se utilizaron por parte de los atacantes para explotarlas. Repasan los lenguajes existentes para representar ataques: P-Best, STATL, LogWeaver, CISL, BRO, Snort Rules e IDMEF y presentan varios escenarios de su con ataques comunes de "Denial of Service – Syn Flood", "The Classic Mitnick Type Attack" y "Buffer Overflow Attack".

4.11 Zhou et al. "An Integrated QoS-Aware Service Development and Management Framework" [37].

El trabajo propone un método de gestión y aseguramiento de la calidad del servicio (*QoS-aware*), que consiste de una infraestructura de gestión *QoS-aware*, una ontología QoS y una ontología de propiedades QoS, entendiendo por servicio como un tipo de funcionalidad que el software puede entregar, desde servicios de información hasta otros más elaborados que tienen impacto en el mundo real. La ontología QoS proporciona un mapa de conocimiento de los conceptos QoS y sus relaciones, para la interacción y comunicación de servicios *QoS-aware*. Mientras, la ontología de propiedades QoS se divide a su vez en dos: ontología técnica QoS y ontología directiva. La primera proporciona los conceptos y relaciones QoS asociados con el desarrollo software, mientras que la segunda se centra en los conceptos QoS y relaciones asociados con la provisión de servicios. Como línea futura pretenden aplicar este desarrollo de software a nivel de la arquitectura.

4.12 Zhou et al. "Ontology Based Software Reliability Modelling" [38].

Se propone un método basado en ontologías para el modelado de fiabilidad en software, el cual incluye una ontología de fiabilidad (y los pasos necesarios para su construcción y mejora), además de un sistema de modelado de fiabilidad basado en ontologías, con el que se facilita a los ingenieros de fiabilidad el conocimiento así como posibles herramientas y entornos de trabajo a utilizar. Dichas ontologías han sido modeladas con OWL y como líneas futuras se pretende ampliar los conceptos y relaciones identificadas en al ontología de fiabilidad y aplicar el método al diseño de arquitecturas software.

5 Resultados

Una vez identificados los estudios primarios y extraída su información relevante en esta sección se presentan los resultados tras realizar su análisis en base a la

clasificación de los estudios y la comparación de las principales propuestas mediante un marco formal de comparación ontológico.

En primer lugar mostramos en la Tabla 2 el resultado final de la clasificación de todos los estudios primarios en función de las diferentes áreas que definimos en la planificación de la revisión. En ella podemos observar como la mayoría de las propuestas actuales están definidas para un dominio concreto, existiendo un menor número de propuestas que intenten definir una ontología de seguridad general. o que estén orientadas a la seguridad a nivel de la web semántica.

Tabla 2. Estudios primarios clasificados por áreas.

Categorías	Referencias	Nº de estudios
Ontologías de seguridad	[4, 12, 17, 24, 25, 27, 37]	7
Ontologías de dominio	[9, 16, 19-22, 30, 34, 36, 38]	10
Teóricos	[3, 11, 18, 31]	4
Seguridad en la Web Semántica	[4, 17, 23, 26, 28, 29, 32, 33, 35]	7
Total		**28**

En segundo lugar se presenta una comparación entre las ontologías de seguridad y del dominio basada en el trabajo presentado en [15], en el que se realiza una medida y comparación general de elementos (conceptos, relaciones, atributos, etc), y otra comparación en base a un subconjunto de las mediciones que se pueden realizar con el marco formal de comparación OntoMetric [39].

No ha sido posible realizar la comparación sobre todas las ontologías identificadas ya que la mayoría no están accesibles por web y al intentar obtenerlas directamente de los autores nos han comunicado que se encuentran en fase de desarrollo, de modo que dejamos como trabajo futuro la incorporación del resto de trabajos cuando estén disponibles. Por otra parte, las conclusiones de cada comparativa se muestran dentro de cada apartado, incluyendo las conclusiones finales en el apartado 6 del documento.

5.1 Comparación general

Para calcular las medidas generales sobre las ontologías de las que disponemos nos hemos ayudado del editor de ontologías en lenguaje OWL, SWOOP[3]. El resultado de la misma se puede ver en la Tabla 3. Hay que tener en cuenta que a la hora de obtener la conclusiones a cada comparativa (tanto la general, como la de Ontometric – sección 5.2), se han tenido en cuenta las ontologías dos a dos, puesto que las dos primeras (la de Denker y Kim) son ontologías descritas a nivel más general y que además tienen aspectos comunes (existe una intersección), ya que ambos definen una ontología para descripción de mecanismos de autentificación; mientras que por otra parte, las ontologías de Dobson y Undercoffer se centran más en dominios específicos como

[3] http://www.mindswap.org/2004/SWOOP

son el de la fiabilidad y los ataques a computadores respectivamente. Más información sobre cada trabajo se puede ver en la sección 4.

En la Tabla 3 podemos observar en las mediciones generales, que el tamaño de la ontología (número de conceptos e instancias) de Denker es superior a la de Kim, por lo que se deduce que la ontología de Kim es mucho más general y no entra en detalles específicos en ninguna de las áreas que intenta modelar. Este hecho destaca aún más, puesto que ontología de Kim esta compuesta de 7 subtonlogías, una de las cuales se centra en mecanismo de autentificación, que Denker describe en mayor profundidad. Sin embargo, Denker no define los conceptos con casi atributos por lo que nos hace pensar que aunque realiza una conceptualización grande del dominio, debería asignar más propiedades a cada concepto como hace Kim.

Por otra parte, las ontologías de Dobson y Undercoffer presentan más conceptos, fruto de que tratan de modelar ontologías para dominios concretos (fialibidad y ataques a computadores respectivamente). Conviene señalar que la ontología de Undercoffer no identifica atributos, por lo que no trata de utilizarlos para definir los conceptos. El resto de medidas de esta comparación general nos van a servir como base para la comparación realizada con Ontometric en la siguiente sección donde se mostrarán las principales conclusiones y resultados.

Tabla 3. Comparación general de ontologías.

	Denker	Kim	Dobson	Undercoffer
Conceptos	87	82	92	106
Conceptos padre	45	20	32	41
Instancias	136	81	61	22
Media de profundidad de la herencia	1,9	2,19	2,26	1,8
Media del nº de conceptos relacionados	0,57	0,37	0,62	0,55
Media del nº de atributos por concepto	0,11	0,42	1,18	0
Media del nº de subclases	0,44	0,65	0,65	0,61
Nº de relaciones taxonómicas	42	62	60	65
Nº de relaciones no taxonómicas	24	25	25	75

5.2 Comparación usando OntoMetric

El método OntoMetric [39] realiza una comparación de características agrupadas en factores que a su vez se agrupan en cinco dimensiones: contenido representado, lenguaje, metodología, entorno software y coste de utilizar la ontología en nuevos sistemas.

En este trabajo nos centramos en el estudio de la dimensión contenido. Por otra parte, en cuanto a la dimensión lenguaje de representación, todas las ontologías que tratamos han sido implementadas mediante OWL.

La dimensión contenido presenta una serie de características descriptivas agrupadas en estos 4 factores: conceptos, relaciones, taxonomía de conceptos y

axiomas. A cada una de estas características se les ha asignado una puntuación de 1 a 5 dependiendo de su grado de cumplimiento, desde muy bajo a muy alto, cuyos valores se observan en las Tablas 4, 5, 6 y 7 y se comentan a continuación.

En el factor conceptos la propuesta de Kim realiza una descripción muy pobre de los conceptos para todo el dominio que quiere abarcar, además que casi no describe los conceptos en lenguaje natural, al contrario que sucede con la de Denker. Por lo tanto, la ontología de Kim dificulta mucho más su reutilización debido a que no se describen en lenguaje natural los conceptos del dominio. Sin embargo, Denker debería asignar más propiedades a cada concepto para así definir bien los atributos que poseen las instancias de dichos conceptos.

En el factor conceptos la propuesta de Undercoffer realiza una descripción muy pobre de los conceptos, además no hace uso de los atributos para describirlos y los identificadores que representan cada concepto en lenguaje natural no son significativos, por lo que complican su entendimiento. Sin embargo, la propuesta de Dobson, hace una descripción más amplia de cada concepto tanto en lenguaje natural como incluyendo atributos que los definen. De esto podemos concluir que la ontología de Dobson es más fácilmente reutilizable que la de Undercoffer.

Tabla 4. Comparación con OntoMetric: factor conceptos.

OntoMetric: factor conceptos	Denker	Kim	Dobson	Undercoffer
Conceptos esenciales	4	2	3	3
Conceptos esenciales en niveles superiores	4	5	5	4
Descripción correcta en lenguaje natural	3	1	3	1
La especificación formal coincide con el lenguaje natural	5	1	5	1
Los atributos describen los conceptos	2	3	4	1
Nº de conceptos	4	2	5	5

Tabla 5. Comparación con OntoMetric: factor relaciones.

OntoMetric: factor relaciones	Denker	Kim	Dobson	Undercoffer
Relaciones esenciales	4	4	4	4
Relacionan los conceptos adecuados	5	5	5	4
Descripción correcta en lenguaje natural	2	1	3	1
Especificación de sus propiedades formales	1	1	2	2
Nº de relaciones	4	4	4	5

En el factor relaciones las ontologías de Kim, y en menor medida la de Denker, destacan por no realizar de forma adecuada la descripción en lenguaje natural de las relaciones y la especificación de sus propiedades formales. Una descripción más formal de las relaciones permitiría su mejor reuso y detección de inconsistencias.

Tanto Undercoffer como Dobson no especifican casi propiedades de las relaciones entre conceptos. Además, como ocurría en los conceptos, Undercoffer no describe las relaciones en lenguaje natural para que sean más fácilmente entendibles y reutilizables.

En el factor taxonomía de conceptos, las ontologías de Kim y Denker carecen del uso de varias perspectivas, de *no_subclase_de* y de *particiones exhaustivas*, por lo que se puede deducir que no proporcionan taxonomías completas. Sería muy recomendable que los autores revisasen que cada clase se descomponga en todas las posibles subclases que pueden ocurrir en el dominio.

De la misma forma, las ontologías de Dobson y Undercoffer carecen de taxonomías completas (particiones exhaustivas apropiadas) como ocurría con las ontologías anteriores.

Las ontologías de Kim y Denker no presentan casi axiomas y por lo tanto el conocimiento que se puede inferir es pequeño. Sin embargo, las ontologías de Dobson y Undercoffer presentan más restricciones que las anteriores y gracias a ellas se puede verificar mejor la consistencia de los conceptos contenidas en ellas. Aun así, sería más recomendable que se incluyesen propiedades formales a las relaciones para verificar su consistencia como son (reflexividad, transitividad, asimetría, simetría, antisimetría y función inversa).

Tabla 6. Comparación con OntoMetric: factor taxonomía de conceptos.

OntoMetric: factor taxonomía de conceptos	Denker	Kim	Dobson	Undercoffer
Varias perspectivas	2	2	4	2
Uso apropiado de no_subclase_de	2	2	1	1
Particiones exhaustivas apropiadas	3	2	2	1
Particiones disjuntas apropiadas	3	4	4	2
Profundidad máxima	3	4	4	3
Media de hijos por concepto	2	3	3	3

Tabla 7. Comparación con OntoMetric: factor axiomas.

OntoMetric: factor axiomas	Denker	Kim	Dobson	Undercoffer
Los axiomas responden consultas	1	1	4	3
Infieren conocimiento	1	1	4	4
Verifican la consistencia	1	1	3	3
Axiomas definidos como conceptos independientes	1	1	1	1
Nº de axiomas	1	1	3	3

6 Conclusiones

Tras haber planificado y ejecutado una revisión sistemática para identificar los principales trabajos ontológicos aplicados a la seguridad y haber analizado y

comparado las principales propuestas, hemos podido observar como la mayoría de ellas están centradas o bien en un dominio de aplicación concreto o bien en la web semántica debido al boom que ha sufrido esta, de modo que podemos afirmar que a día de hoy aún no se ha conseguido por parte de la comunidad científica una ontología general de seguridad. Aunque si se ha detectado que esto es una necesidad dentro de la comunidad de la seguridad.

Dentro de cualquier comunidad científica la creación de una ontología es un factor principal ya que de este modo damos un soporte formal al conocimiento manejado en base a conceptos y relaciones a la vez que mejoramos su compartición. En el campo de la seguridad la formalización de todos los conceptos sería inviable de modo que la definición de una ontología general de seguridad no debería de partir de cero sino que debería de alimentarse e incorporar las propuestas anteriores, a la vez que debería ser flexible y facilitar la realización de actualizaciones que reflejen los cambios y la continua aparición de nuevos conceptos.

Por otra parte, hemos comprobado que los trabajos que integran ontologías y seguridad se encuentran en sus fases iniciales ya que la mayor parte de las propuestas de ontologías de seguridad identificadas no eran accesibles y estaban en estado de desarrollo, por lo que imposibilitaba la comparación. Dentro de las que estaban disponibles para comparación hemos comprobado que en general utilizan pocos atributos para describir los conceptos, con lo cual algunas propiedades de los conceptos no quedan reflejadas; muchas veces las expresiones utilizadas en lenguaje natural para describir los conceptos y relaciones entre ellos no son las idóneas complicando su entendimiento; no son exhaustivas al no recoger todas las posibilidades dentro de un dominio, identificado esto como trabajo futuro en todas ellas; y no utilizan apenas axiomas ni propiedades formales como reflexividad, transitividad, asimetría, simetría, antisimetría y función inversa que permitan inferir conocimiento. Esto conduce a concluir que estas ontologías no están preparadas para poder hacer una rápida integración de conceptos y así poderse reutilizar o integrar entre ellas, aspecto fundamental dentro de la ingeniería ontológica y que permitiría obtener la necesidad detectada de una ontología general y completa de seguridad [3].

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. Devanbu, P. and S. Stubblebine, *Software engineering for security: a roadmap*. ACM Press. Future of Software Engineering, 2000: p. 227-239.
2. Ferrari, E. and B. Thuraisingham. *Secure Databases Systems*. in *Advanced Databases: Technology Design*. 2000. Artech Huse: London.

3. Mouratidis, H. and P. Giorgini, *An Introduction*, in *Integrating Security and Software Engineering: Advances and Future Visions*. 2006, Idea Group Publishing.
4. Denker, G., L. Kagal, and T. Finin, *Security in the Semantic Web using OWL*. Information Security Technical Report, 2005. **10**(1): p. 51-58.
5. Dhillon, G. and J. Backhouse, *Information system security management in the new millennium*. Communications of the ACM, 2000. **43**(7): p. 125-128.
6. 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.
7. Gruninger, M. and J. Lee, *Ontology Applications and Design*. Communications of the ACM, 2002. **45**(2): p. 39-41.
8. 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.
9. 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.
10. 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.
11. Donner, M., *Toward a Security Ontology*. IEEE Security and Privacy, 2003. **1**(3).
12. 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**.
13. Biolchini, J. and P. Gomes, *Systematic Review in Software Engineering*. 2005, Systems Engineering and Computer Science Department, UFRJ: Río de Janeiro, Brazil.
14. 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.
15. 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.
16. 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.
17. Denker, G., et al., *Security for DAML Web Services: Annotation and Matchmaking*, in *The SemanticWeb - ISWC 2003*. 2003, Springer Berlin / Heidelberg. p. 335-350.
18. 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.
19. 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.
20. 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.
21. Geneiatakis, D. and C. Lambrinoudakis, *An ontology description for SIP security flaws*. Computer Communications, 2006. **In Press, Corrected Proof**.
22. 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.
23. Kagal, L. and T. Finin, *Modeling conversation policies using permissions and obligations*. AAMAS workshop on Agent communication, LNCS. Springer-Verlag, 2005.

24.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.
25.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.
26.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**.
27.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.
28.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.
29.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.
30.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.
31.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.
32.Tan, J.J. and S. Poslad, *Dynamic security reconfiguration for the semantic web*. Engineering Applications of Artificial Intelligence, 2004. **17**(7): p. 783-797.
33.Thuraisingham, B., *Security standards for the semantic web*. Computer Standards & Interfaces, 2005. **27**(3): p. 257-268.
34.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.
35.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.
36.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.
37.Zhou, J., E. Niemela, and P. Savolainen, *An Integrated QoS-Aware Service Development and Management Framework*. wicsa, 2007: p. 13.
38.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.
39.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).