AVANCES EN CRIPTOLOGÍA Y SEGURIDAD DE LA INFORMACIÓN

Benjamín Ramos Álvarez
Arturo Ribagorda Garnacho
(Directores)

RECSI VIII
REUNIÓN ESPAÑOLA SOBRE CRIPTOLOGÍA Y SEGURIDAD DE LA INFORMACIÓN

IAZ DE ANTOS

Benjamín Ramos Álvarez
Arturo Ribagorda Garnacho
(Directores)

AVANCES EN CRIPTOLOGÍA Y SEGURIDAD DE LA INFORMACIÓN

Co-Directores:
Julio C. Hernández Castro
José M.ª Sierra Cámara

DIAZ DE SANTOS

Benjamín Ramos Álvarez
Arturo Ribagorda Garnacho
(Directores)

AVANCES EN CRIPTOLOGÍA Y SEGURII DE LA INFORMACIÓN

Co-E
Julio C. Hérnán
José M.ª Sier

IAZ DE ANTOS

Ediciones Díaz de Santos, S. A.
Doña Juana I de Castilla, 22
28027 MADRID
www.diazdesantos.es/ediciones
ediciones@diazdesantos.es

ISBN: 84-7978-650-5
Depósito legal: M. 37.746-2004

Diseño de Cubierta:
Fotocomposición e impresión: Fernández Ciudad, S. L.
Encuadernación: Rústica-Hilo, S. L.

Impreso en España

AGRADECIMIENTOS

Una reunión científica como esta que nos ocupa no podría celebrarse sin la co confianza de diversas personas y entidades. Por ello es de justicia que el Comité agradezca a todos ellos su colaboración y en especial a los organismos y empresas trocinado esta RECSI'04: Ministerio de Educación y Ciencia, Universidad Carl drid, Computer Associates, Accenture, Revista SIC, Criptored y Secnware. Así mis debemos agradecer la colaboración de Zona Multimedia en el diseño gráfico.

ÍNDICE DE CAPÍTULOS

Parte II
CRIPTOANÁLISIS

Parte III
PROTOCOLOS CRIPTOGRÁFICOS Y VALIDACIÓN

Parte IV
SEGURIDAD EN SISTEMAS DE INFORMACIÓN (BD, aplicaciones, etc.)

Parte V
SEGURIDAD EN REDES E INTERNET

Parte VI
SERVICIOS DE CERTIFICACIÓN Y NOTARIZACI

Parte VII
SEGURIDAD EN DRM

Anexos
UNA VISIÓN EMPRESARIAL

40

INCORPORANDO SEGURIDAD AL MODEL MULTIDIMENSIONAL

Rodolfo Villarroel[1], Eduardo Fernández-Medina[2], Juan Trujillo[3], M
[1] Departamento de Computación e Informática, Universidad Católica
Avenida San Miguel 3605
Talca (Chile)
Teléfono: 56 71 203525, Fax: 56 71 260278
rvillarr@spock.ucm.cl
[2] Departamento de Informática, Universidad de Castilla-La M
Paseo de la Universidad, 4
13071 Ciudad Real (España)
Teléfono: +34 926 29 53 00, Fax: +34 926 29 53 54
{Eduardo.FdezMedina, Mario.Piattini}@uclm
[3] Departamento de Lenguajes y Sistemas Informáticos, Universidad
Apartado de correos, 99. 03080
San Vicente. C.P. 03690 Alicante (España)
Teléfono: +34 96 590 34 00 ext. 2967, Fax +34 96 590 93
jtrujillo@dlsi.ua.es

Resumen. En la actualidad hay un campo maduro en relación a metodologías y técnic
lado multidimensional (MD), sin embargo, hay un campo inmaduro en considerar asp
estas metodologías y técnicas. La seguridad de la información es un serio requisite
cuenta, no como un aspecto aislado, sino como un elemento presente en todas las eta
el caso de la confidencialidad de la información, se debe asegurar que los usuarios p
información que les otorgan sus privilegios. En modelos MD, la confidencialidad es e
información de negocio, que es muy sensible, puede ser descubierta ejecutando una
mentablemente las metodologías que incorporan seguridad se basan en un entorno op
co, por lo tanto carecen de enfoques de modelado MD para trabajar con Data Wareh
Datos MD y aplicaciones de Procesamiento Analítico en Línea (OLAP). Este articul
sión basada en el Lenguaje de Modelado Unificado (UML) para modelado MD que p
mentos de seguridad en una aplicación MD por medio de los mecanismos estándares d
Finalmente, se muestra un ejemplo con la aplicación de la extensión.

1. INTRODUCCIÓN

La seguridad es definida por diversos autores [5, 13] como la capacidad de
software para proteger los datos e información de manera que personas o sis
zados no puedan leerlos o modificarlos y que el acceso no sea denegado a p
do. Esta capacidad debería estar presente en todo el proceso de desarrollo
embargo, la seguridad de los sistemas de información se considera una vez
desarrollado. Este enfoque es conocido como "Penetrate and Patch" (penetrar
el cual se ha comprobado que tiene malos resultados. Las soluciones se han
palmente en proveer defensas de seguridad (tales como firewalls, routers, ser
guración, password y cifrado) en vez de resolver uno de los principales aspect
problemas de seguridad, que se refiere a un apropiado diseño de software [7].

Afortunadamente, han surgido nuevas metodologías que incorporan la seguridad en sus procesos de desarrollo [6, 14, 19, 21]. Cada una de estas metodologías tiene aspectos muy interesantes respecto a seguridad, que pueden servir como base para cubrir aspectos no contemplados en nuevas metodologías o extensiones que sean generadas. En [28] se ha realizado una comparativa de estas propuestas de integración de seguridad en el modelado, y se ha observado que a la vez, estas metodologías tienen una serie de limitaciones, una de las cuales se refiere a que enfocan la seguridad sólo en sistemas que trabajan en un entorno operacional y no analítico. Estos entornos tienen diferentes funciones. Si deseáramos manejar, para propósitos de análisis y toma de decisiones, información consistente, integrada, bien definida y dependiente del tiempo, nos daremos cuenta que los datos disponibles en los sistemas operacionales no cumplen con tales requisitos. Para solucionar este problema se debe trabajar en un entorno analítico fuertemente apoyado por el uso de modelos MD para diseñar DW. Un DW es "una colección de datos orientados al tema, integrados, no volátiles e historiados, organizados para que sirvan de apoyo a la toma de decisiones" [12]. Esta definición indica que los datos no se orientan por procesos funcionales, propios de las aplicaciones clásicas, sino por temas, proporcionando una visión única e integrada de la organización, que se concibe de forma transversal. Además, la información no es tratada de manera estática, sino que cobra importancia la evolución de la misma a lo largo del tiempo.

Además, en la literatura, podemos encontrar diversas iniciativas para incluir seguridad en DW, bases de datos MD y aplicaciones OLAP [2, 4, 15, 17, 24, 25]. Muchas de ellas se enfocan en aspectos interesantes relacionados con el control de acceso, seguridad multinivel, su aplicación a bases de datos federadas, aplicaciones usando herramientas comerciales, etc. Sin embargo, ninguna de ellas estudia los aspectos de seguridad considerando todas las etapas del ciclo de desarrollo de sistemas ni considera la introducción de seguridad en el diseño MD. Como no existe un enfoque metodológico que integre la seguridad en el diseño MD, podemos establecer que este problema sigue sin ser resuelto. Además de aplicar un enfoque metodológico, sería deseable que los sistemas que se construyan, si éstos almacenan datos personales o sensibles, cumplan con los requisitos necesarios de protección. En muchos países estos requisitos vienen ya exigidos y determinados por la existencia de leyes en materia de protección de datos personales (por ejemplo, La Ley Orgánica de Protección de Datos de Carácter Personal en el caso de España [1]).

En la siguiente sección haremos una propuesta de extensión de seguridad, basada en UML, para el modelado conceptual MD. Esta propuesta será descrita junto a un ejemplo. Finalmente, estableceremos las conclusiones y líneas futuras de trabajo a partir de este artículo.

2. PROPUESTA DE MODELADO DE SEGURIDAD MULTIDIMENSIONAL

En esta sección se describe la técnica de modelado conceptual MD orientada a objetos de la que hemos partido, y posteriormente se describen las extensiones para seguridad en el modelado de DW, para finalmente proporcionar un ejemplo que clarifique los conceptos tratados en nuestra propuesta.

2.1. Modelado Conceptual Multidimensional Orientado a Objetos

Hay mucho trabajo realizado en relación a las metodologías y técnicas asociac lado de DW, bases de datos MD y aplicaciones OLAP [10, 16, 26, 27]. Sin hay mucho trabajo en relación a la integración de aspectos de seguridad en las as y técnicas de este tipo de modelado. Algunas propuestas de seguridad asoc han sido desarrolladas pero son soluciones puntuales que cumplen parcialmente tos de seguridad. Además, ninguna de estas propuestas considera un enfoque m de manera formal que incluya la seguridad en el proceso de diseño MD.

En este trabajo, nos basamos en un enfoque de modelado MD que utiliza diante un perfil formado por un conjunto de estereotipos de UML) para rep propiedades estructurales de los modelos MD [20, 27]. En la Tabla 40.1 se forma resumida los estereotipos para clases y atributos definidos junto a una br ción y el icono correspondiente para facilitar su uso e interpretación.

Tabla 40.1. Estereotipos para clases y atributos

Nombre	Tipo	Descripción
Fact	Clase	Clases de este estereotipo representan hechos en un modelo MD.
Dimension	Clase	Clases de este estereotipo representan dimensiones en un modelo MD.
Base	Clase	Clases de este estereotipo representan niveles de jerarquía de dimensiones en un modelo MD.
OID	Atributo	Atributos de este estereotipo representan atributos *OID* de clases de *hecho*, *dimensión* o *base* en un modelo MD.
FactAttribute	Atributo	Atributos de este estereotipo representan atributos de clases de *hecho* en un modelo MD.
Descriptor	Atributo	Atributos de este estereotipo representan atributos *descriptor* de clases *dimensión* o *base* en un modelo MD.
DimensionAttribute	Atributo	Atributos de este estereotipo representan atributos de clase *dimensión* o clase *base* en un modelo MD.

Las propiedades estructurales del modelado MD se representan mediante un de clases en el que la información se organiza en hechos y dimensiones. Los he dimensiones se representan mediante *clases de hecho* (estereotipo *Fact*) y *clases sión* (estereotipo *Dimension*) respectivamente. Las clases de *hecho* se definen co compuestas en una relación de agregación de *n* clases de dimensión. La cardinali ma en el rol de las clases de dimensión es *1* para indicar que todo hecho ha de ésta relacionado con todas las dimensiones. Las relaciones "muchos a muchos" entre y una dimensión en particular se especifican mediante la cardinalidad *1..** en el clase dimensión correspondiente. Un hecho se compone de medidas o atributos (estereotipo *FactAttribute*). Por defecto, todas las medidas en una clase de *hechos* deran aditivas. Las medidas semiaditivas y no aditivas se especifican mediante r nes. Además, también se pueden representar medidas derivadas (mediante la restri

sus reglas de derivación se especifican entre llaves alrededor de la clase de hechos correspondiente, como muestra la Figura 40.1 (a).

Este enfoque OO también permite la definición de atributos identificadores (estereotipo *OID*). También se pueden representar "dimensiones degeneradas" [8, 16], lo que proporciona otras características a los hechos además de las medidas definidas. Con respecto a las dimensiones (estereotipo *Dimension*), cada nivel de una jerarquía de clasificación se representa mediante una *clase base* (estereotipo *Base*). Una asociación de clases *base* especifica una relación entre dos niveles de una jerarquía de clasificación. El único prerrequisito es que estas clases deben definir un Grafo Acíclico Dirigido a partir de la *clase de dimensión* (restricción {dag} definida en el estereotipo *Dimension*). La restricción {dag} permite representar tanto las jerarquías múltiples como las de camino alternativo. Cada clase *base* debe contener un atributo *identificador* (estereotipo *OID*) y un atributo *descriptor* (estereotipo *Descriptor*), además de los atributos adicionales propios que caracterizan a las instancias de dicha clase.

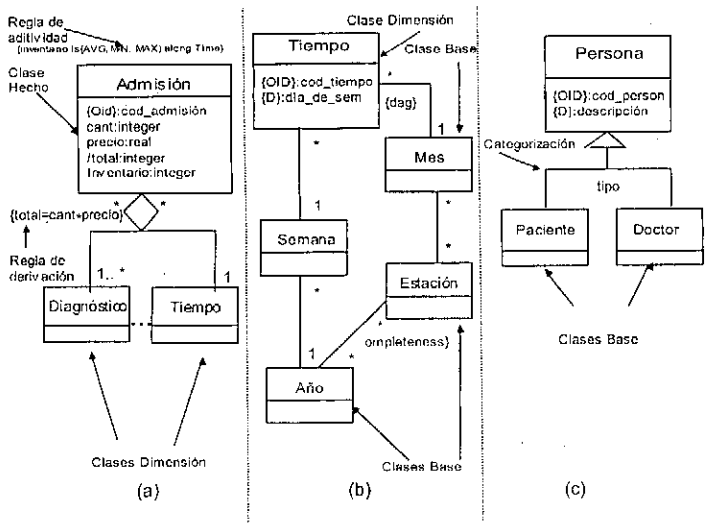

Figura 40.1. Modelado MD usando UML.

Se puede apreciar en la Figura 40.1 que la principal propiedad estructural del modelado MD es el diagrama de clases, donde se separa la información en hechos y dimensiones. Las clases de *hecho* son especificadas como clases compuestas en relaciones de agregación compartidas de clases de dimensión. En el ejemplo de la Figura 40.1 (a) la clase de *hecho* es *Admisión* y las clases de *dimensión* son *Diagnóstico* y *Tiempo*. Si se considera una dimensión como *Tiempo*, en la Figura 40.1 (b) se puede observar que existe una jerarquía de clasificación, que incluso puede tener vías alternativas. Se puede también observar en la Figura 40.1 (c) la categorización de la dimensión Persona, por medio del uso de relaciones de generalización y especialización.

2.2. Extensiones para la Seguridad en el Modelado Multidimensiona

Basado en el modelado MD presentado y en los tipos de restricciones a proponen los siguientes mecanismos de extensión para el modelado conc

- Valores Etiquetados: Este tipo de extensión permitirá indicar el que tiene la información en una clase de *hecho*, clase de *dime* Cada etiqueta de seguridad podrá almacenar información relati sibilidad de la información, a roles de usuarios y a distintas c cionales de información. A medida que el nivel de seguridad s será el nivel de sensibilidad. Los roles de usuarios serán neces ganización en la que se implante el DW sea demasiado grande pación de los usuarios del DW en grupos organizados jerárqui llamaremos roles) que tengan diferentes funciones en la organiz to que tengan acceso a determinados datos. Las categorías per áreas que describirán la sensibilidad de un dato etiquetado, per dato con una o varias áreas organizacionales con diferencias de
- Restricciones: Son especificadas usando el lenguaje OSCL [cialmente diseñado para especificar restricciones de seguridad. guaje de restricciones es posible especificar tanto las restriccion modelo como todas aquellas que se refieran a diferentes necesi lidad para los distintos componentes del modelo.

El proceso de integración de seguridad en modelos MD consistirá por lo

- Definir la organización de los usuarios que tendrán acceso al s mos definir un nivel preciso de granularidad considerando tres zación de usuarios: Niveles de seguridad (que indica el nivel d usuario), Categorías de usuario (que indica una clasificación h rios) y Roles de usuario (que indica una organización jerárqui acuerdo a sus roles o responsabilidades dentro de la organización
- Asignar niveles, categorías y roles a los elementos del modelo d características. Podemos definir para cada elemento del model clase de *dimensión*, atributo de *hecho*, etc.) su información de una tupla que está compuesta de una secuencia de niveles de seg to de categorías de usuario y un conjunto de roles de usuario.
- Especificar restricciones de seguridad considerando la informac La información de seguridad y restricciones indican las propied que los usuarios deben poseer para poder acceder a la informació

Podemos identificar, y especificar con complejas restricciones OSCL m formadas (que por razones de espacio no hacemos). Estas reglas son agru

- Relaciones entre la información de seguridad de las clases y sus
  - Los niveles de seguridad definidos para un atributo tienen q restrictivos que los niveles de seguridad definidos para su cl gla es aplicable para las jerarquías de roles y categorías de us

- La información de seguridad de las instancias:
  - El nivel de seguridad de la instancia de una clase tiene que estar incluida en el intervalo de niveles de seguridad que han sido definidas para la clase. La misma regla es aplicable para las instancias de atributos.
  - Los roles de usuario para una instancia de una clase, tiene que ser un subárbol del árbol de roles que han sido definidas para la clase. La misma regla es aplicable para la instancia de los atributos.
  - Las categorías de usuario de una instancia de una clase, tiene que ser un subconjunto de las categorías que han sido definidas para la clase. La misma regla es aplicable para la instancia de los atributos.
- Categorización de dimensiones:
  - Cuando una clase de *dimensión* es especializada en varias clases *base*, los niveles de seguridad de las subclases tienen que ser igual o más restrictivos que los niveles de seguridad de la superclase. La misma regla es aplicable para jerarquía de roles y categorías de usuarios.
- Jerarquías de clasificación. Como regla general, podemos considerar que mientras más específica sea la información, más restringido es su acceso.
  - Si la clase A tiene una asociación 1..* con la clase B, significa que la información de A agrupa a la información de B, tal que B es más específico que A. El nivel de seguridad definido para la clase B tiene que ser más restrictivo que el nivel de seguridad definido para la clase A. Esta regla también es aplicable para roles de usuario y categorías.
  - Si la clase A tiene una asociación *..* con la clase B, el diseñador tiene que decidir que clase contiene la información más específica.
- Atributos derivados:
  - Los niveles de seguridad de un atributo derivado tienen que ser igual o más restrictivos que el atributo del cual éste es derivado. La misma regla es aplicable para roles de usuarios y categorías. Por defecto, un atributo derivado hereda la información de seguridad del atributo del cual procede.
- Combinación de dimensiones:
  - Una consulta a la clase de *hecho* tiene que considerar la información de seguridad que ha sido definida para esa clase.
  - Una consulta que involucra la combinación de una clase de *dimensión* (o puede ser una clase *base*) y la clase de *hecho* tiene que considerar la combinación de la información de seguridad de la clase *dimensión* (o *base*) y de la clase *hecho*. Los niveles de seguridad de la combinación serán más restrictivos que los niveles de seguridad de la clase *dimensión* (o *base*) y la clase *hecho*. La misma regla es aplicable para los roles de usuario y categorías.
  - Una consulta que involucra la combinación de varias clases de *dimensión*, y la clase de *hecho*, tiene que considerar la combinación de la información de seguridad de todas las clases. Los niveles de seguridad de la combinación será el más restrictivo de los niveles de seguridad de todas las clases. La misma regla es aplicable para los roles de usuarios y categorías.

2.3. Ejemplo de Aplicación del Modelado de Seguridad

El caso de estudio se relaciona con la admisión de pacientes de un hospital. El ejemp una adaptación de ejemplos presentados en [3, 9]. La admisión de pacientes está co clase de *hecho* de nombre *Admisión*, las clases de *dimensión* de nombres *Diagnóstico*, *po* y *Edad*, y las clases *base* que aparecen en la Figura 40.2.

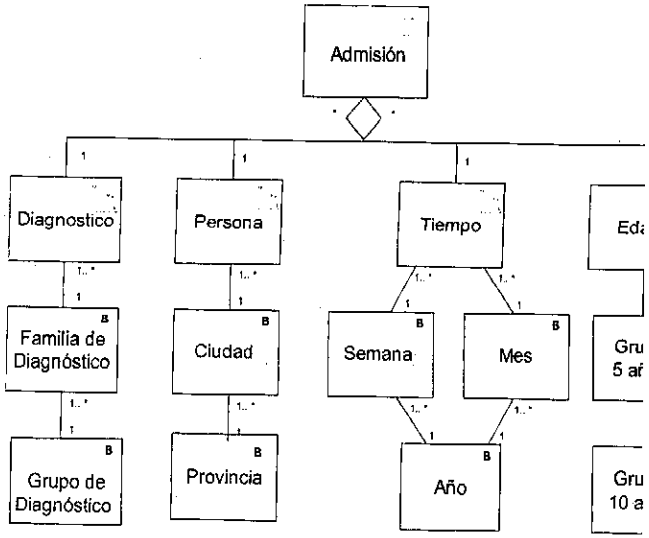

Figura 40.2. Modelado MD para admisión de pacientes.

Como pueden existir muchos diagnósticos en una clasificación, éstos son agr clases base *Familia de Diagnóstico* y *Grupo de diagnóstico*. Por ejemplo, el dia abetes dependiente de la insulina *durante el embarazo*" es parte de la familia " *rante el embarazo*" y éste a la vez es parte del grupo "*Diabetes*". La dimensió gistra los datos personales, incluyendo el lugar de residencia, el cual es parte d que a la vez es parte de una región. La dimensión Tiempo contiene atributos cor al día, y de manera jerárquica se pueden obtener información correspondiente año o mes y año. La dimensión Edad permite establecer una jerarquía de atributo

Con el objetivo de mostrar el problema que nos preocupa de una manera n hemos seleccionado una parte del modelo mostrado en la Figura 40.2 y lo hen y ampliado con sus atributos y aspectos de seguridad (Figura 40.3). Esta figur restricciones de seguridad para la clase de *hecho* y las clases de *dimensión D Paciente*. El nivel de sensibilidad (valor etiquetado *SL o SecurityLevels*) apli ejemplo considera los siguientes valores: *A=Alto Secreto*, *S=Secreto*, *C=Co P=Público*. Se utiliza, además, un conjunto de roles de usuario (valor etiq *SecurityRoles*). La jerarquía de roles para este ejemplo es:

- *phosp = personal de hospital*
  - *Psalud = personal de salud*
    - *doctor*
    - *enfer = enfermero*
  - *admin = administrativo*
  - *paciente*

En el nivel superior de la jerarquía se podrán asignar permisos generales, poco relevantes, que podrán ser heredados por los niveles de menor jerarquía. En este caso, la asignación de permisos al rol *psalud permitirá que esos privilegios sean heredados por* los roles *doctor* y *enfer*. Además, existen diferentes categorías organizacionales (valor etiquetado *SC* o SecurityCompartments), en este ejemplo, *medi=medicina interna* y *neum=neumología*. El ejemplo muestra que hay algunos atributos que tienen un rango de niveles (ejemplo: el atributo descripción tiene el rango de niveles S..A, lo cual significa que una restricción a través de OSCL deberá especificar cuando se aplica el nivel *Secreto* (*S*) o el nivel *Alto Secreto* (*A*). El establecimiento de restricciones en OSCL para la clase de *hecho Admisión* y clase de *dimensión Diagnóstico* puede ser observada mediante notas en notación UML. Por ejemplo, la restricción OSCL asociada a los niveles de seguridad (*self.SL*), indica que a partir de un coste determinado asociado a la admisión, el nivel de seguridad será más restrictivo (pasará de *Secreto* a *Alto Secreto*). Otra restricción en OSCL, en este caso para la dimensión *Diagnóstico*, que nos permite especificar que los enfermos con ciertas enfermedades tendrán más protegidos sus datos para que no pueda ser violada su privacidad, esta restricción en OSCL está asociada a los roles (*self.securityroles*) que son asignados para el acceso a la información. Para este ejemplo, sólo los doctores manejarán la información de enfermos de cáncer o sida. Al tener denegada la información respecto a estas enfermedades en esa dimensión, tampoco podrá tener acceso a la clase de *hecho* la cual permitiría no sólo obtener las medidas almacenadas, sino que también permitirá el acceso por medio de los hechos a las demás dimensiones (como por ejemplo, los datos personales).

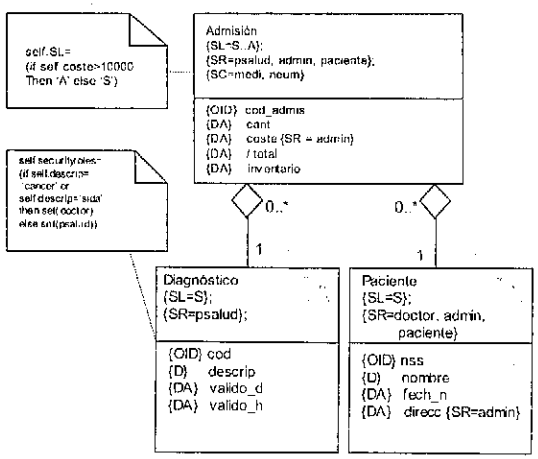

Figura 40.3. Restricciones de seguridad en el modelado MD.

Además, en este ejemplo, podemos ver que un usuario puede cumplir quisitos para acceder la clase de *dimensión Diagnóstico*, pero puede no clase de *hecho Admisión*, debido a que este acceso es restringido, además, En este caso, el usuario debería tener privilegios en las categorías *medi* (y *neum* (neumología). Una de las restricciones inherentes es que el u privilegios en todas las categorías de la clase.

3. CONCLUSIONES Y TRABAJO FUTURO

Muchas de las metodologías existentes que incorporan seguridad en el pr llo de sistemas de información no consideran las características propias d co, propio de los DW, bases de datos MD y aplicaciones OLAP. A la ve: as que consideran el modelado MD, no incorporan aspectos de seguridad Se ha planteado como solución una extensión basada en UML para ir ridad en el modelado MD. Proveemos a UML, con las ventajas que esto terísticas de seguridad para ser capaz de incluir en los modelos que incluy: y potencia de UML y por otro lado las nuevas características de segurid usadas, cuando la aplicación incluya requisitos de seguridad que necesite ticas. La aplicación de esta extensión ha permitido generar una especifica que no era contemplada en el modelado MD. Además, el uso de esta exte implementación de modelos MD seguros con algunos de los Sistemas de de Datos (SGBD) que tienen la capacidad para implementar bases de dato como Oracle Label Security [18] y DB2 Universal Database [11].

A corto y medio plazo, el trabajo futuro se dedicará a la definición de para el modelado MD, y a la construcción de una metodología completa l en el Proceso Unificado, para desarrollar DW seguros que garanticen l información y que ayuden al cumplimiento de las leyes existentes sobre pr de carácter personal.

Agradecimientos

Esta investigación es parte de los proyectos CALIPO (TIC2003-(RETISTIC (TIC2002-12487-E), soportados por la Dirección General de Ministerio de Ciencia y Tecnología, y la red VII-J.RITOS2 financiada por

Referencias

[1] *Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Perso 14/12/1999*. 1999..

[2] A. Abelló, M. Oliva, J. Samos, y F. Saltor. *Information Systems Architecture for Secu* En *3rd. Workshop on Engineering Federated Information Systems (EFIS2000)*. 2000. I

[3] T. Bach y C. Jensen. *Multidimensional Data Modeling for Complex Data*. En *15th Inte on Data Engineering (ICDE'99)*. 1999. Sydney, Australia.

[4] B. Bhargava. *Security in Data Warehousing (Invited Talk)*. En *2nd International Warehousing and Knowledge Discovery (DAWAK'00)*. 2000. London, U.K.: Springer.

[5] S. Castano, M. Fugini, G. Martella, y P. Samarati, *Database Security*. 1995: Addison-W

[6] E. Fernández-Medina y M. Piattini. *Designing Secure Database for OLS.* En *Database and Expert Systems Applications: 14th International Conference (DEXA 2003).* 2003. Prague, Czech Republic: Springer.
[7] A. Ghosh, C. Howell, y J. Whittaker. *Building Software Securely from the Ground Up.* IEEE Software, 2002. 19(1): p. 14-16.
[8] W. Giovinazzo. *Object-Oriented Data Warehouse Design. Building a star schema.* 2000. New Jersey, USA: Prentice-Hall.
[9] M. Golfarelli, D. Maio, y S. Rizzi. *Conceptual Design of Data Warehouses from E/R Schemes.* En *32th Hawaii International Conference on Systems Sciences (HICSS 1998).* 1998. Hawaii, USA: IEEE Computer Society.
[10] M. Golfarelli y S. Rizzi. *A Methodological Framework for Data Warehouse Design.* En *1st International Workshop on Data Warehousing and OLAP (DOLAP'98).* 1998. Maryland, USA.
[11] IBM. *Security: IBM to provide multilevel security on the zSeries mainframe.* 2004.
[12] H. Inmon. *Building the Data Warehouse.* Tercera edición. 2002, USA: John Wiley & Sons.
[13] ISO/IEC. *ISO/IEC 15408-1. Information Technology. Security Techniques. Evaluation Criteria for TI Security. Part I: Introduction and General Model.* 1999: Switzerland.
[14] J. Jürjens. *UMLsec: Extending UML for secure systems development.* En *UML 2002 - The Unified Modeling Language, model engineering, concepts and tools,* J. Jézéquel, H. Hussmann, y S. Cook, Editores. 2002, Springer: Dresden, Germany. p. 412-425.
[15] N. Katic, G. Quirchmayr, J. Schiefer, M. Stolba, y A. Min Tjoa. *A Prototype Model for Data Warehouse Security Based on Metadata.* En *9th International Workshop on Database and Expert Systems Applications (DEXA'98).* 1998. Vienna, Austria.: IEEE Computer Society.
[16] R. Kimball, L. Reeves, M. Ross, y W. Thornthwaite. *The Data Warehousing Lifecycle Toolkit.* 1998, New York, USA: John Wiley & Sons.
[17] R. Kirkgöze, N. Katic, M. Stolda, y A. Min Tjoa. *A Security Concept for OLAP.* En *8th International Workshop on Database and Expert System Applications (DEXA'97).* 1997. Toulouse, France: IEEE Computer Society.
[18] J. Levinger. *Oracle label security. Administrator's guide. Release 2 (9.2).* 2002: http://www.csis.gvsu.edu/GeneralInfo/Oracle/network.920/a96578.pdf
[19] L. Liu, E. Yu, y J. Mylopoulos. *Security and Privacy Requirements Analysis within a Social Setting.* En *11th International Requirements Engineering Conference.* 2003: IEEE Computer Society.
[20] S. Luján-Mora, J. Trujillo, y I.Y. Song. *Extending the UML for Multidimensional Modeling.* En *5th International Conference on the Unified Modeling Language (UML 2002).* 2002. Dresden, Germani: Springer-Verlag.
[21] D. Marks, P. Sell, y B. Thuraisingham. *MOMT: A multi-level object modeling technique for designing secure database applications.* Journal of Object-Oriented Programming, 1996. 9(4): p. 22-29.
[22] G. McGraw. *Penetrate and Patch is Bad.* IEEE Software, 2002: p. 15-15.
[23] M. Piattini y E. Fernández-Medina. *Specification of security constraints in UML.* En *35th Annual 2001 IEEE International Carnahan Conference on Security Technology.* 2001. London, United Kingdom.
[24] T. Priebe y G. Pernul. *Towards OLAP Security Design - Survey and Research Issues.* En *3rd ACM International Workshop on Data Warehousing and OLAP (DOLAP'00).* 2000. Washington DC, USA.
[25] A. Rosenthal y E. Sciore. *View Security as the Basis for Data Warehouse Security.* En *2nd International Workshop on Design and Management of Data Warehouse (DMDW'00).* 2000. Sweden.
[26] C. Sapia, M. Blaschka, G. Höfling, y B. Dinter. *Extending the E/R Model for the Multidimensional Paradigm.* En *1st International Workshop on Data Warehouse and Data Mining (DWDM'98).* 1998. Singapore: Springer-Verlag.
[27] J. Trujillo, M. Palomar, J. Gómez, y I.Y. Song. *Designing Data Warehouses with OO Conceptual Models.* IEEE Computer, special issue on Data Warehouses, 2001(34): p. 66-75.
[28] R. Villarroel, E. Fernández-Medina, y M. Piattini. *A Comparison of Secure Information Systems Design Methodologies.* En *Ninth CAiSE/IFIP8.1/EUNO International Workshop on Evaluation of Modeling Methods in Systems Analysis and Design.* 2004. Riga, Latvia.

41

INTEGRANDO LA INGENIERÍA DE SEGURID PROCESO DE INGENIERÍA SOFTWARI

Antonio Maña, Diego Ray, Francisco Sánchez, Mariemma
Departamento de Lenguajes y Ciencias de la
Computación de la Universidad de Málaga
email: {amg, diego, cid, yague}@crypto.lcc.uma.es

Resumen. Las técnicas de Ingeniería del Software actuales han evolucionado creciente complejidad de las nuevas aplicaciones software. Pero en esta concerniente a la seguridad ha sido erróneamente considerada como suplen técnicas de ingeniería de seguridad no están integradas dentro del proceso de sino que son añadidas una vez que el software está casi finalizado. Además, la se basa normalmente en métodos formales y altamente teóricos que n relacionados con el software en desarrollo, lo cual tiene consecuencias muy n de los sistemas desarrollados de esa forma. Por otra parte, las herramientas de están basadas fundamentalmente en notaciones gráficas sin una semántica pr propiedades y requisitos relacionados con la seguridad. Este artículo present trabajo con el objetivo de definir e implementar una metodología y un marco d herramientas automatizadas que permita el desarrollo de aplicaciones y sistema es crítica. En particular, este artículo describe los mecanismos que permite procesamiento automático de los requisitos de seguridad en los modelos softwa en UML.

1. INTRODUCCIÓN

Cada día los proyectos software se van haciendo más extensos y más co que a menudo comprenden múltiples divisiones o incluso la totalidad d aplicaciones basadas en la web están comenzando a usarse de forma ma web se están convirtiendo en elementos clave en esas aplicaciones, fabricantes, proveedores, socios, compradores y vendedores comun Teniendo en cuenta la creciente complejidad de los proyectos softw *Ingeniería de Software* han evolucionado para hacer frente a esas nuev objetivos como reutilización, flexibilidad o independencia de la plata sólo algunos aspectos fundamentales.

Algunas de estas aplicaciones, tales como sistemas de objetos dis web o computación grid, pueden representar pasos fundamentales en Internet. Sin embargo, la ausencia de seguridad y de mecanismos de c está obstaculizando su desarrollo. Los requisitos de seguridad son crí tales como los de comercio electrónico y trabajo colaborativo. La adecuadas que permitan garantizar que los sistemas y aplicaciones p problemas de seguridad asociados, representa en la práctica una barrera el desarrollo extendido de esas aplicaciones.

* Trabajo parcialmente desarrollado en el proyecto europeo CASENET No. IST-2001-324