Patrocinadores

Entidades Organizadoras

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

ISBN: 978-84-9732-595-0

CEDI 2007 XII Jornadas de Ingeniería del Software y Bases de Datos | JISBD'07 |

CEDI 2007

II CONGRESO ESPAÑOL DE INFORMÁTICA

ZARAGOZA SPAIN

AUDITORIO PALACIO DE CONGRESOS
11 AL 14 DE SEPTIEMBRE DE 2007

XII Jornadas de Ingeniería del Software y Bases de Datos

| JISBD'07 |

EDITOR
Xavier Franch

ACTAS DE LAS XII JORNADAS DE INGENIERÍA DEL SOFTWARE Y BASES DE DATOS

EDITOR

Xavier Franch

PATROCINA

InterSystems

COLABORA

THOMSON

ACTAS DE LAS XII JORNADAS DE INGENIERÍA DEL SOFTWARE Y BASES DE DATOS (JISBD'07)

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

ISBN: 978-84-9732-595-0
Depósito legal: M-

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

IMPRESO EN ESPAÑA-PRINTED IN SPAIN

Comité Ejecutivo

Presidente del Comité de Programa

Xavier Franch (Universitat Politècnica de Catalunya)

Secretario de la Comisión Permanente

Mario Piattini (Universidad de Castilla-La Mancha)

Coordinadora de Tutoriales

Ana M. Moreno (Universidad Politécnica de Madrid)

Coordinador de Talleres

Vicente Pelechano (Universidad Politécnica de Valencia)

Coordinador de Demostraciones

Antonio Vallecillo (Universidad de Málaga)

Coordinador de la Sesión de Divulgación de Trabajos Relevantes ya Publicados

Oscar Díaz (Universidad del País Vasco)

Composición y Maquetación de Actas

Jordi Marco (Universitat Politècnica de Catalunya)

Organización y Relaciones con CEDI 2007

Fran J. Ruiz (Universidad de Zaragoza)
M. Elena Gómez (Universidad de Zaragoza)
Javier Tuya (Universidad de Oviedo)

Comité Organizador

Presidente del CEDI

Alberto Prieto (Universidad de Granada)

Presidente del Comité Ciéntifico

Juan J. Moreno (Universidad Politécnica de Madrid)

Presidente del Comité Organizador CEDI 2007

Victor Viñals (Universidad de Zaragoza)

Coordinador de Actividades Plenarias CEDI 2007

José Duato (Universidad Politécnica de Valencia)

Secretario del CEDI 2007

José A. Castellanos (Universidad de Zaragoza)
José A. Bañares (Universidad de Zaragoza)

Comité de Programa

Alberto Abelló, Univ. Polit. Catalunya
Silvia Abrahão, Univ. Polit. Valencia
Jesus Aguilar, Univ. Sevilla
José Aldana, Univ. Málaga
Bárbara Álvarez, Univ. Polit. Cartagena
María J. Aramburu, Univ. Jaume I
João Araújo, Univ. Nova de Lisboa
Orlando Belo, Univ. do Minho
Rafael Berlanga, Univ. Jaume I
Pere Botella, Univ. Polit. Catalunya
Nieves Brisaboa, Univ. Coruña
Isabel S. Brito, Inst. Polit. Beja
Coral Calero, Univ. Castilla-La Mancha
Carlos Canal, Univ. Málaga
José M. Cavero, Univ. Rey Juan Carlos
Matilde Celma, Univ. Polit. Valencia
Rafael Corchuelo, Univ. Sevilla
Dolors Costal, Univ. Polit. Catalunya
Yania Crespo, Univ. Valladolid
Oscar Dieste, Univ. Polit. Madrid
Javier Dolado, Univ. País Vasco
João Falcão e Cunha, Univ. Porto
Pablo de la Fuente, Univ. Valladolid
Lidia Fuentes, Univ. Málaga
Mario Gaspar da Silva, Univ. Lisboa
Marcela Genero, Univ. Castilla-La Mancha
Cristina Gómez, Univ. Polit. Catalunya
Jaime Gómez, Univ. Alicante
Alfredo Goñi, Univ. País Vasco
Juan Hernández, Univ. Extremadura
Jon Iturrioz, Univ. País Vasco
Natalia Juristo, Univ. Polit. Madrid
Patricio Letelier, Univ. Polit. Valencia
Antonia Lopes, Univ. Lisboa
Adolfo Lozano, Univ. Extremadura
Esperanza Marcos, Univ. Rey Juan Carlos
Eduardo Mena, Univ. Zaragoza
Ana Moreira, Univ. Nova de Lisboa
Juan J. Moreno, Univ. Polit. Madrid
Juan M. Murillo, Univ. Extremadura
Oscar Pastor, Univ. Polit. Valencia
Antonio Polo, Univ. Extremadura
Carme Quer, Univ. Polit. Catalunya
Celia Ramos, Univ. Algarve
Isidro Ramos, Univ. Polit. Valencia
José Riquelme, Univ. Sevilla
Antonio Rito, Univ. Técnica de Lisboa
Antonio Ruíz, Univ. Sevilla
Francisco Ruíz, Univ. Castilla-La Mancha
José Samos, Univ. Granada
Fernando Sánchez, Univ. Extremadura
Juan Sánchez, Univ. Polit. Valencia
Ernest Teniente, Univ. Polit. Catalunya
Miguel Toro, Univ. Sevilla
Ambrosio Toval, Univ. Murcia
Juan C. Trujillo, Univ. Alicante
Javier Tuya, Univ. Oviedo
Belén Vela, Univ. Rey Juan Carlos
Cristina Vicente, Univ. Polit. Cartagena

Comité Asesor para la Selección de Trabajos de Prestigio

Oscar Díaz (Presidente), Univ. País Vasco
Alan Davis, Univ. of Colorado
Neil A.M. Maiden, City Univ. London
Timos Sellis, Nat. Technical Univ. Athens

Revisores Adicionales

César J. Acuña
Amaia Aguirregoitia
Diego Alonso
David Benavides
Jordi Cabot
Paloma Cáceres
Javier Cámara
Dante Carrizo
Pedro J. Clemente
Jose M. Conejero
Javier Cubo
Norberto Díaz
Amador Durán
Sergio España
Mauricio Espinoza
Ismael Etxeberria
Antonio Fariña
Raul Fernandez
L. Fredlund
Antonielly Garcia
Antonio Cesar Gómez
Ángel Herranz
Sergio Ilarri
Miguel Ángel Laguna
Maria Lencastre
Marta López
Francisco Javier Lucas
María Esperanza Manso
Julio Mariño
José Manuel Marqués
Francisco Martínez
Jorge Martínez
Miguel Ángel Martínez
Fernando Molina
Ana M. Moreno
Elena Navarro
Ismael Navas
Isabel Nepomuceno
Juan A. Nepomuceno
Joaquín Nicolás
Guadalupe Ortiz
Juan Angel Pastor
Joaquin Peña
Jenifer Pérez
Juan Manuel Pérez
Beatriz Pontes
Álvaro Prieto
Antonia M. Reina
Domingo Savio Rodríguez
Roberto Rodríguez
Oscar Romero
Fran J. Ruiz
Angeles Saavedra
Gwen Salaün
Pedro Sánchez
André L. Santos
Diego Seco
Jesús Serrano
Encarna Sosa
Toufik Taibi
Raquel Trillo
José Antonio Troyano
Juan Manuel Vara

Sistema Automático de Revisión

Quercus Software Engineering Group

Jose Javier Berrocal Universidad de Extremadura

Conferencia auspiciada por

Prólogo

Respondiendo a su cita anual, las XII Jornadas de Ingeniería del Software y Bases de Datos (JISBD) se han celebrado en Zaragoza, entre el 11 y el 14 de septiembre de 2007. Las Jornadas representan un punto de encuentro de la comunidad investigadora en ingeniería del software y en bases de datos. En sus inicios se celebraron dos eventos diferenciados, las Jornadas de Ingeniería del Software y las Jornadas sobre Investigación y Docencia en Bases de Datos. Posteriormente, en 1999, ambos eventos se unificaron en uno solo, reflejando la interrelación existente entre estas disciplinas. En esta duodécima edición, las Jornadas han constituido, una vez más, un punto de encuentro en el que profesionales y académicos de España, Portugal y Latinoamérica, de ambos campos, han podido compartir experiencias y resultados entre distintos grupos de investigación, desarrollo e innovación tecnológica.

Actualmente, JISBD es un evento auspiciado por Sociedad de Ingeniería del Software y Tecnologías de Desarrollo de Software (SISTEDES, http://www.sistedes.org). Entre los fines de dicha organización destacan el de promover la investigación, la innovación y la transferencia de tecnología entre los distintos agentes involucrados en el avance las tecnologías del Software y el de fomentar actividades con otras asociaciones nacionales e internacionales con fines similares, consiguiendo así proporcionar una mayor visibilidad a la investigación de sus asociados.

Al igual que en 2005, las XII Jornadas de Ingeniería del Software y Bases de Datos se han realizado en el marco del II Congreso Español de Informática (CEDI 2007). Esto ha permitido a los participantes de las Jornadas participar en las diversas actividades de CEDI de interés para toda la comunidad de investigación en Informática, tales como conferencias invitadas y mesas redondas. La celebración cada dos años de JISBD en el marco de CEDI encaja con los objetivos citados de dicha organización.

Este volumen recoge los trabajos seleccionados por el Comité de Programa de JISBD'07. Se recibieron un total de 87 contribuciones de 9 países: España, Portugal, Argentina, Brasil, Chile, Colombia, Cuba, México y Venezuela. Cada contribución fue revisada por tres miembros del Comité de Programa. Posteriormente, se abrió una fase de discusión en la que se debatieron en mayor profundidad algunos trabajos y eventualmente se pidieron revisiones adicionales para ellos; asimismo, algunos trabajos se aceptaron condicionalmente, pendientes de verificar que la versión definitiva trataba adecuadamente los comentarios de los revisores; gracias al esfuerzo de los autores, todos estos trabajos fueron finalmente aceptados. Como resultado de todo el proceso, se configuró un programa compuesto por 30 artículos. Adicionalmente, se seleccionaron 5 trabajos más para su presentación como artículos cortos. Además, en esta edición de JISBD se recogió la posibilidad de presentar trabajos ya publicados en foros de prestigio reconocido. Se seleccionaron 4 artículos de esta modalidad. Finalmente, destacamos la celebración de una sesión para la presentación de herramientas, cuya convocatoria tuvo una acogida excelente por parte de la comunidad de JISBD, de manera que en dicha sesión se programaron un total de 19 demostraciones de herramientas.

El día previo a la conferencia, se organizaron un total de 7 talleres y un tutorial. Estos eventos están ganando importancia a cada nueva edición de JISBD y en el caso de los talleres, están creando sus propias comunidades con intereses más específicos. Algunos talleres ya están plenamente consolidados y llegan a acumular hasta un total de 8 ediciones. Cabe destacar que a partir de este año, las actas de los talleres se recogen en una publicación única en formato electrónico, con el soporte de SISTEDES, para potenciar la difusión de los trabajos presentados.

En referencia al programa, mencionar la participación de dos conferenciantes invitados de reconocido prestigio, siguiendo la pauta de ediciones anteriores. La primera conferencia impartida por Stephen Mellor, miembro del Object Management Group, y con un largo historial en la formulación de métodos para el análisis orientado a objetos. La segunda conferencia a cargo del profesor

John Mylopoulos, que posee igualmente una dilatada experiencia en diversos ámbitos de la ingeniería del software. La presencia de estos dos investigadores representó un elemento importante en el programa de las Jornadas.

Quisiera destacar un hecho que no por obvio, deja de ser merecedor de mención. La celebración de un evento de las características de JISBD, con una participación cada vez más numerosa y consolidada, y con unas exigencias de calidad que se van incrementando en cada edición, no podría realizarse sin la dedicación totalmente desinteresada de un gran número de personas. Desde el punto de vista científico, el trabajo en equipo desarrollado por los miembros del Comité Ejecutivo, en cuyo seno se han debatido los temas más candentes en la configuración de la oferta científica del congreso; y por supuesto la ardua y puntual labor de revisión efectuada por los miembros del Comité de Programa y los revisores adicionales. Desde el punto de vista organizativo, destacar la gran dedicación de los miembros del Comité Ejecutivo responsables de las tareas de enlace con CEDI, y la labor del Grupo Quercus de Ingeniería del Software de la Universidad de Extremadura, quienes han estado a cargo de todo el sistema de recepción y revisión de artículos. También deseo agradecer el soporte recibido por las entidades patrocinadoras y colaboradoras, y en especial la labor de respaldo de SISTEDES, tanto por lo que se refiere a apoyo logístico como a tareas de difusión, como ya se ha comentado. Y por último, especialmente, a los autores de los trabajos enviados a JISBD'07, en definitiva son ellos los que hacen posible la celebración del evento.

Finalmente, desear que el volumen que ahora tienes en tus manos, y que refleja el estado del arte en la investigación en Ingeniería del Software y Bases de Datos en la comunidad de habla hispana y portuguesa, sea de utilidad para tu trabajo.

Zaragoza, Septiembre 2007
Xavier Franch (editor)

Índice

CONFERENCIAS INVITADAS

TUTORIAL

TRABAJOS RELEVANTES YA PUBLICADOS

DESARROLLO DE SOFTWARE DIRIGIDO POR MODELOS

PROCESOS

ARTÍCULOS CORTOS

DEMOSTRACIONES

ALMACENES Y MINERÍA DE DATOS

PRUEBAS DEL SOFTWARE

TECNOLOGÍAS DE BASES DE DATOS

LÍNEAS DE PRODUCTO. ORIENTACIÓN A ASPECTOS

REQUISITOS. METAMODELADO EN MEDICIÓN

MODELIZACIÓN CONCEPTUAL DE DATOS

ARQUITECTURAS SOFTWARE

MODELOS DE CALIDAD

Especificación de Procesos de Negocio Seguros a través de una extensión de UML 2.0

Alfonso Rodríguez
Departamento de Auditoría e Informática
Universidad del Bio Bio
Chillán
Chile
alfonso@ubiobio.cl

Eduardo Fernández-Medina
Mario Piattini
Grupo de investigación ALARCOS
Departamento de Tecnologías y Sistemas de Información
Universidad de Castilla-La Mancha
Ciudad Real, España
{Eduardo.FdezMedina,Mario.Piattini}@uclm.es

Juan Trujillo
Departamento de Lenguajes y Sistemas Informáticos
Universidad de Alicante
Alicante
España
jtrujillo@dlsi.ua.es

Resumen

Los procesos de Negocio (BP) son un recurso importante para el desempeño y la mantención de la competitividad en las empresas. Para representar procesos de negocio, en los últimos años se han mejorado lenguajes y han aparecido nuevas notaciones. La importancia de la seguridad en el desempeño de los procesos de negocio es ampliamente aceptada. No obstante, la perspectiva del experto del negocio en relación con la seguridad ha sido escasamente tratada. En este artículo presentamos una extensión del Diagrama de Actividad de UML 2.0 que permite especificar requisitos de seguridad en BP. Para ello hemos usado el mecanismo de extensibilidad de UML, compuesto por estereotipos, restricciones y valores etiquetados. También hemos usado OCL para especificar las restricciones. Hemos aplicado nuestra propuesta en un ejemplo de un proceso de negocio típico para la admisión de pacientes en una institución de salud.

1. Introducción

Un modelo es una vista simplificada de una realidad compleja. Es una manera de crear una abstracción, que permita, al mismo tiempo, eliminar los detalles irrelevantes y centrarse en los aspectos importantes. También debe facilitar el intercambio de puntos de vista entre los diversos interesados en el negocio orientando el trabajo hacia objetivos comunes [4].
En el modelado de proceso de negocio el objetivo principal es producir una descripción de la realidad que permita entenderla y eventualmente modificarla con el propósito de incorporar mejoras. Para ello, es importante contar con una notación que permita modelar con la mayor claridad posible la esencia del negocio.
Hoy en día, y de acuerdo con el estado de la industria del modelado de BP [16], es posible identificar a Unified Modeling Language (UML) [19] y Business Process Modeling Notación (BPMN) [3] como los estándares más importantes. Aunque ambos son aceptados en el ámbito de los negocios, el modelado con UML es dominante en la industria del software. Esto último, permitiría pasar desde las especificaciones de procesos de negocio hasta modelos más concretos.
Paralelamente, los ingenieros de software están fuertemente influenciados por la arquitectura dirigida por modelos (MDA, Model Driven-Architecture) [18], un nuevo paradigma que apunta a trabajar en el nivel de modelos y metamodelos. MDA es un marco de trabajo en que debe ser posible (i) hacer una especificación de un sistema independiente de la plataforma que lo va a soportar, (ii) especificar plataformas, (iii) seleccionar una determinada plataforma para el sistema y (iv) transformar la especificación del sistema en una especificación para una plataforma en particular.
Por otra parte, aunque se reconoce la importancia de la seguridad, ésta ha sido a menudo descuidada en el modelado de procesos de negocio, ya que usualmente se han concentrado en el modelado del proceso propiamente dicho [2]. Esto se debe a que el experto en el dominio del proceso de negocio no es un especialista en seguridad [9]. Tampoco los ingenieros de requisitos están entrenados del todo en seguridad y los pocos que han sido

Actas de las XII Jornadas de Ingeniería del Software y Bases de Datos, JISBD'2007, pp.336-345 ISBN: 978-84-9732-595-0

entrenados, sólo tienen una idea general de los mecanismos de la arquitectura de seguridad, tales como claves de acceso y encriptación, en lugar de los requisitos reales de seguridad [5]. Adicionalmente, la identificación de requisitos de seguridad ha sido confusa ya que por lo general se tiende a identificar *requisitos funcionales de seguridad*. Este tipo de requisitos varía dependiendo del tipo de aplicación. En cambio, los *requisitos de seguridad* no varían en un alto nivel de abstracción. La razón es que en ese nivel la valoración y vulnerabilidad de los activos es la misma [6].

En este artículo presentamos una extensión del Diagrama de Actividad de UML 2.0 (UML 2.0-AD) mediante la cual se podrá especificar requisitos de seguridad en el dominio del negocio. Este trabajo completa y mejora la propuesta presentada en [24]. Además, hemos enmarcado esta propuesta en un contexto de creación software utilizando MDA como marco de referencia y vinculando los artefactos que se obtienen de la especificación de seguridad en procesos de negocio con algunos flujos de trabajo del Proceso Unificado (UP, Unified Process) [11, 23]. Hemos extendido UML porque es (i) ampliamente utilizado en la industria del software, (ii) tiene mecanismos de extensibilidad que están claramente definidos y (iii) en esta última versión ha mejorado la representación de procesos de negocio.

El resto del artículo se encuentra organizado de la siguiente forma: en la Sección 2 presentaremos los principales trabajos relacionados con la especificación de requisitos de seguridad en procesos de negocio y extensiones de UML 2.0-AD, en la Sección 3 mostraremos la manera en que nuestra propuesta se enmarca en el ámbito de MDA. En la Sección 4 describiremos de manera detallada la extensión que proponemos, en la Sección 5 mostraremos un ejemplo ilustrativo y, finalmente, en la Sección 6 presentaremos nuestras conclusiones.

2. Trabajos relacionados

En esta sección presentamos la revisión de los trabajos relacionados con la especificación de seguridad en procesos de negocio y las extensiones que se han propuesto para el diagrama de actividad de UML 2.0.

Hemos encontrado trabajos en que se relaciona la seguridad en forma directa con el concepto de proceso de negocio [9, 10, 25]. En esas propuestas se incorpora la *perspectiva de proceso de negocio* en relación con la definición de seguridad. Dichas propuestas se complementan con el uso de COPS (COmercial Protocols and Service), una infraestructura con la que es posible construir mercados electrónicos adaptables y $MoSS_{BP}$ (Modeling Security of Business Process) que da soporte al dominio de los expertos del negocio que no requieren ser expertos en seguridad. En [2], los autores ponen especial atención en la incorporación de criptografía como requisito de seguridad. Para ello usan un enfoque basado en el refinamiento por etapas que amplían agregando la especificación de requisitos de seguridad y modelos de confianza. Esto da origen a una especificación con seguridad que luego se transformará en especificaciones refinadas que tienen incorporada la seguridad. Finalmente en [17, 28] se propone un marco de trabajo basado en UML para representar la semántica de seguridad en un entorno de desarrollo integrado que incluye los procesos de negocio y el modelado de sistemas. Este enfoque tiene la ventaja de integrar los requisitos de seguridad como otros requisitos en el contexto del desarrollo de software.

Por su parte los trabajos relacionados con extensiones de UML 2.0-AD y procesos de negocio se refieren a: (i) aspectos del negocio tales como consumidores, tipos de procesos de negocio, metas, despacho de productos y medidas relacionadas con conceptos del negocio [15], (ii) metas de procesos y medidas de desempeño que se hacen conceptualmente visibles y que proveen una correspondencia especificada en BPEL para hacer disponibles las medidas de ejecución y monitoreo [13], (iii) un almacén de datos y su relación con la estructura dinámica de los procesos de negocio [26], (iv) la agregación de semántica a los actividades para que consideren aspectos organizacionales que permitan poner restricciones durante la ejecución de las actividades [12] y (v) una definición más formal de la semántica de UML 2.0-AD basada en la metodología original de flujos de señales [27].

No obstante, la diversidad de trabajos que usan UML para hacer especificaciones de seguridad y las extensiones propuestas para UML 2.0-AD, no hay en la literatura una extensión de UML 2.0 en que se incorpore requisitos de seguridad en el Diagrama de Actividad.

3. Modelado de Procesos de Negocio Seguros en el ámbito de MDA

En el último tiempo se está poniendo especial atención en la transformación de modelos. MDA, en particular, está orientado a resolver los problemas de tiempo, costes y calidad asociados con la creación de software. Este enfoque está compuesto por (i) una perspectiva independiente de computación que considera un punto de vista del entorno del sistema (ii) una perspectiva independiente de plataforma que considera un punto de vista de la operación del sistema sin especificar detalles de la plataforma y (iii) una perspectiva que tiene que ver con una plataforma específica [18]. Los principales elementos de MDA se presentan en la Figura 1 (adaptada de [8]).

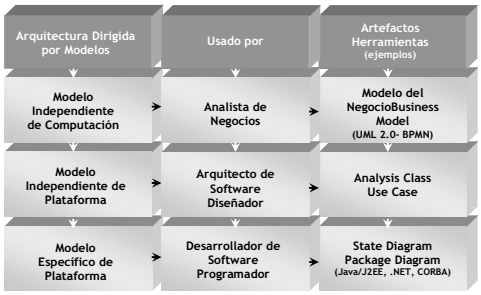

Figura 1: Secuencia de desarrollo MDA

En la Figura 2 se muestran, en color gris oscuro, la extensión de UML 2.0-AD, que hemos llamado BPSec (Business Process Security), las reglas QVT para la transformación de modelos, el proceso de negocio seguro (SBP, Secure Business Process) y la herramienta BPSec-Tool que hemos diseñado para especificar un SBP y obtener los artefactos UML en forma automática.

En el ámbito de MDA, el uso de la extensión permite hacer especificaciones independientes de computación (Modelo SBP) y pasar, por medio de transformación de modelos, hacia especificaciones independiente de plataforma (clases de análisis y casos de uso). En la última columna de esta figura hemos incorporado las flujos de trabajo del proceso unificado. El objetivo es mostrar que tanto la especificación del SBP como las clases de análisis y casos de uso pueden ser utilizados en forma complementaria en un proceso de desarrollo de software consolidado y exitoso. De esta forma, el modelo SBP será usado en la etapa de "Modelo del Negocio" y las clases de análisis y los casos de uso se usarán en las etapas de "Requisitos" y "Análisis & Diseño".

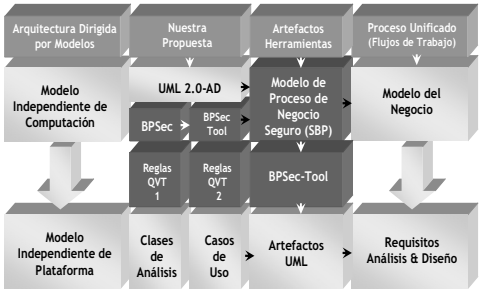

Figura 2: Nuestra propuesta

Las transformaciones para obtener clases de análisis han sido descritas usando QVT y las trasformaciones que permiten obtener casos de uso se obtienen aplicando reglas QVT, reglas de refinamiento y listas de chequeo.

Para llevar cabo la especificación de un SBP y automatizar las transformaciones hemos desarrollado una herramienta que llamamos BPSec-Tool. Esta herramienta ha sido construida usando una arquitectura de tres capas en que se separan los componentes relacionados con la presentación, aplicación y almacenaje. Para el desarrollo de estos componentes usamos MS-Visio, C#, y MS-Access respectivamente.

Tanto las transformaciones como descripción de la herramienta se encuentran fuera del ámbito de este artículo.

4. BPSec: la extensión del Diagrama de Actividad de UML 2.0

El diagrama de actividad es el elemento de UML 2.0 que se usa para representar procesos de negocio y flujos de trabajo [12, 22].

El metamodelo de UML 2.0-AD, condensado de la especificación presentada en [19, 21], se muestra en la Figura 3. *Activity* es el elemento central para representar un proceso de negocio. Se relaciona con *ActivityGroup*, *ActivityNode* y *ActivityEdge* a través de una asociación de composición. Dicha relación se extiende a las clases *Action, ActivityPartitition, Interrruptible ActivityRegion, DataStoreNode* y *ObjectFlow*.

En relación con la definición de lenguajes para diferentes dominios, OMG (Object Management

Group), contempla dos enfoques. El primero basado en la definición de un nuevo lenguaje, como una alternativa a UML, y el segundo enfoque se basa en la especialización de UML. Este último, llamado perfil (profile), se usa para proporcionar una: (i) terminología que se adapte una plataforma o dominio específico, (ii) sintaxis adicional para constructores que no tiene una determinada notación, (iii) notación distinta a la que ya existe agregando símbolos o semántica que no este especificada en el metamodelo [19].

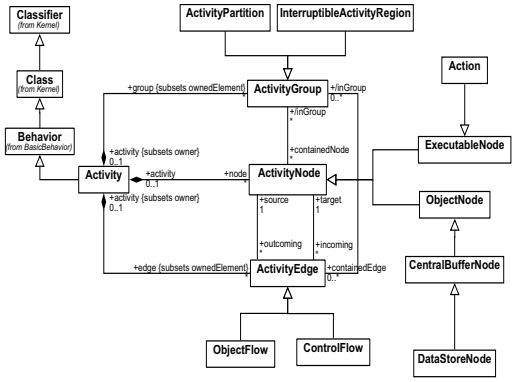

Figura 3: Metamodelo de UML 2.0-AD

Un perfil está compuesto de estereotipos, restricciones y valores etiquetados. Un estereotipo es un elemento del modelo definido por su nombre y la clase base desde la cual es heredado. Las restricciones se aplican a los estereotipos con el propósito de indicar limitaciones (por ejemplo, pre-condiciones, post-condiciones o invariantes). Estas restricciones pueden ser expresadas en lenguaje natural, lenguaje de programación o un lenguaje especializado como OCL (Object Constraint Language) [20]. Los valores etiquetados son meta atributos adicionales que se especifican como un par nombre-valor.

En cuanto a los requisitos de seguridad, estos deben permitir expresar a los expertos de negocios ciertas limitaciones o restricciones en relación a determinados elementos que componen un proceso de negocio. Esta perspectiva debe estar exenta de tecnicismos propios de la implementación de la seguridad en sistemas software, ya que, de otro modo no se podría considerar como parte de un modelo independiente de computación.

Tradicionalmente se han identificado tres objetivos de seguridad: confidencialidad, integridad y disponibilidad y más recientemente se ha agregado autenticación [7]. También es posible usar clasificaciones que consideren secreto, integridad, disponibilidad y responsabilidad [14] o aspectos tales como autorización, auditoría, anonimato y separación de deberes [1].

En este trabajo consideraremos definiciones de requisitos de seguridad que sean comprensibles para los analistas de negocios y no ambiguas para los expertos en seguridad. Hemos tomado como referencia la taxonomía propuesta en [6]. Desde allí hemos seleccionado un subconjunto de requisitos tomando en cuenta (i) la claridad de la definición, (ii) el potencial significado en el ámbito de los negocios y (iii) la medida en que la definición no esté relacionada con soluciones específicas de seguridad. El subconjunto, no limitado, de requisitos de seguridad que utilizaremos en nuestra propuesta está compuesto por: control de acceso, detección de ataques y amenazas, auditoría de seguridad, integridad, no repudio y privacidad (Access Control, Attack Harm Detection, Security Auditing, Integrity, Non repudiation y Privacy).

Para la representación de estos requisitos de seguridad en procesos de negocio definidos con UML 2.0-AD, hemos definido BPSec. Este perfil está compuesto por diecisiete estereotipos: uno que especializa la clase *Activity*, doce que especializan a la clase *Element (from Kernel)* y cuatro que especializan la clase *Enumeration (from BasicBehavior)*. En la Figura 4, se muestra la parte del metamodelo de UML con la cual se relacionan los estereotipos que proponemos. En esa figura los nuevos estereotipos se muestran en gris y los elementos del metamodelo de UML se muestran color blanco.

El estereotipo «SecureActivity» especializa a la clase *Activity* de manera que el nuevo estereotipo conserva las relaciones de *Activity* (ver Figura 3). «SecureActivity» debe estar compuesta por al menos un requisito de seguridad. Esto permite establecer la relación de los requisitos de seguridad con los elementos de UML 2.0-AD. El estereotipo «SecurityRequirement» agrupa los estereotipos «AccessControl», «AttackHarm Detection», «Integrity», «NonRepudiation» y «Privacy» que representan los requisitos de seguridad. El estereotipo «AuditRegister» ha sido especializado en «NR-AuditRegister», «SP-AuditRegister» y «G-AuditRegister». Tanto

«SecurityRole» como «SecurityPermission» complementan las especificaciones de seguridad. Finalmente, los estereotipos «RequirementType», «PermissionOperation», «ProtectionDegree» y «PrivacyType» son tipos de datos que permiten especificar características propias de los requisitos de seguridad que conforman el perfil.

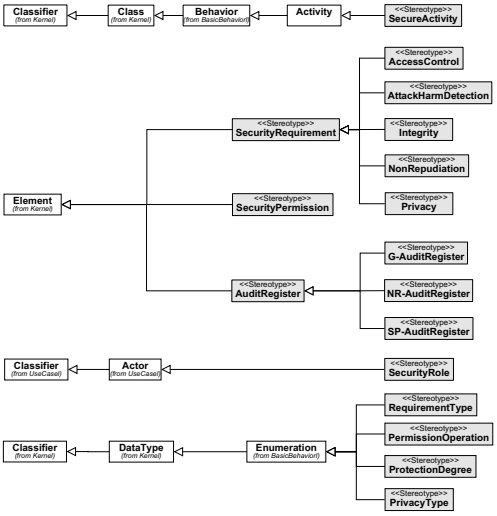

Figura 4: Estereotipos de BPSec

En la Figura 5 se muestran una vista general de los paquetes que conforman la especificación de la extensión. En el paquete Type BPSec se encuentran los tipos de datos en que se definen permisos de operación, tipos de privacidad, grados de protección y tipos de requisitos. Estos tipos de datos componen el espacio de BPSec lo que permitirá utilizarlos como valores etiquetados en los estereotipos. El elemento más importante del paquete BPSec el estereotipo «SecureActivity» que especializa a la clase *Activity*.

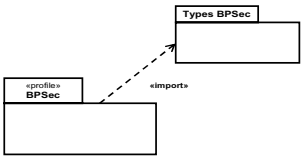

Figura 5: Vista general del perfil BPSec

En la Figura 6 se muestra el modelo de los estereotipos que componen de BPSec (en color gris). Además se puede ver la relación que tienen estos estereotipos con los elementos de UML 2.0-AD sobre los cuales se puede especificar requisitos de seguridad.

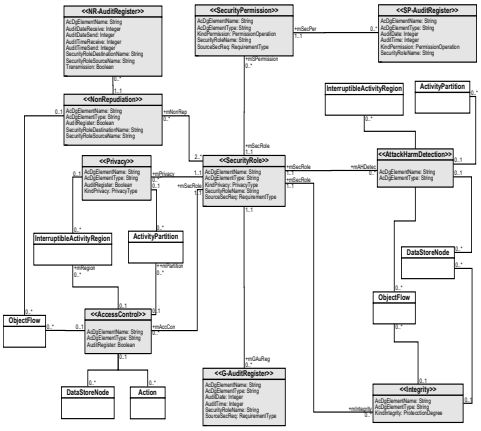

Figura 6: Relación entre UML 2.0-AD y BPSec

Debido a que esta extensión no necesita hacer referencia a extensiones previas, sólo mostraremos una descripción detallada de los estereotipos y tipos de datos. Para cada estereotipo especificaremos nombre, generalización (clase base), descripción, asociaciones con otros estereotipos o clases UML, notación, valores etiquetados y restricciones. Los estereotipos que componen BPSec, se describen en orden alfabético en forma detallada en la Tabla 1.

Tabla 1 Descripción de los estereotipos

Nombre: **AccessControl**

Generalización: SecurityRequirement

Descripción: Corresponde a la limitación de acceso a recursos sólo a usuarios autorizados. La especificación de este requisito por parte del analista de negocios implica la limitación de acceso a un conjunto de recursos que son valorados como importantes de ser protegidos de manera especial. Desde la perspectiva de la seguridad esta especificación supone la definición de roles que pueden ser asignados a personas, entidades, programas, dispositivos u otros sistemas y la definición de permisos para acceder a los objetos que se encuentran en el ámbito de la especificación de control de acceso. Este requisito adicionalmente puede tener una especificación de registro de auditoría

Asociaciones: Action[0..*], ActivityPartition[0..*], DataStoreNode[0..*], InterruptibleActivityRegion[0..*], ObjectFlow[0..*], SecurityRole[1..1]

Notación: 

Valores Etiquetados: AcDgElementName, AcDgElementType, AuditRegister

Restricciones

1. La especificación de control de acceso da origen a permisos de seguridad asociados con los elementos que se encuentran en el ámbito de la especificación de control de acceso
   context AccessControl
   inv: self.mSRole.mSPermission→size()=1
2. La especificación de registro de auditoría genera un estereotipo «G-AuditRegister» relacionado con el rol de seguridad y un estereotipo «SP-AuditRegister» relacionados con los permisos y los objetos en el ámbito de la especificación de control de acceso.
   context AccessControl

inv: self.AuditRegister=True implies (self.G-AuditRegister→size()>=1 and self.SP-AuditRegister→size()>=1)

3. El nombre del rol de seguridad que se genera a partir de una especificación de control de acceso que se hizo sobre Action, DataStoreNode u ObjectFlow deberá ser el mismo nombre de la partición o región que los contiene.
   context AccessControl
   inv: if self.Action→size()=1 then
   self.interruptibleRegion→size()>=1 implies
   self.mSRole.SecurityRoleName=self.interruptibleRegion.Name
   else
   self.inPartition→size>=1 implies
   self.mSRole.SecurityRoleName=self.inPartition.Name
   endif
   inv: if self.DataStoreNode→size()=1 then
   self.interruptibleRegion→size()>=1 implies
   self.mSRole.SecurityRoleName=self.interruptibleRegion.Name
   else
   self.inPartition→size>=1 implies
   self.mSRole.SecurityRoleName=self.inPartition.Name
   endif
   inv: if self.ObjectFlow→size()=1 then
   self.interrups→size()>=1 implies
   self.mSRole.SecurityRoleName=self.interrups.Name
   else
   self.inPartition→size()>=1 implies
   self.mSRole.SecurityRoleName=self.inPartition.Name
   endif
4. Cuando exista una doble especificación de control de acceso, el rol de seguridad tomará el nombre de la partición o región que lo contenga
   context AccessControl
   inv: self.ActivityPartition→size()>1 and
   (self.Action→size()=1 or self.DataStoreNode→size()=1 or
   self.ObjectFlow→size()=1) implies
   self.mSRole.SecurityRoleName=self.mPartition.Name
   inv: self.InterruptibleActivityRegion→size()>1 and
   (self.Action→size()=1 or self.DataStoreNode→size()=1 or
   self.ObjectFlow→size()=1) implies
   self.mSRole.SecurityRoleName=self.mRegion.Name

Nombre: **AttackHarmDetection**

Generalización: SecurityRequirement

Descripción: Se define como la detección, registro y notificación de una tentativa de ataque y amenaza, ya sea que tenga éxito o fracase. Desde la perspectiva del analista de negocios, este requisito representa una señal de atención sobre los elementos en que se indica. También se puede interpretar como un paso previo a una especificación de control de acceso. Desde el punto de vista de la seguridad esta especificación implica mantener un registro de los eventos (ataques y amenazas) ocurridos sobre elementos potencialmente vulnerables. Este requisito sólo puede ser especificado con registro de auditoría

Asociaciones: ActivityPartition[0..*], DataStoreNode[0..*], InterruptibleActivityRegion[0..*], ObjectFlow[0..*], SecurityRole[1..1]

Notación: 

Valores Etiquetados: AcDgElementName, AcDgElementType

Restricciones

1. Cuando de se especifique detección de ataques y amenazas se debe crear un rol de seguridad y un registro de auditoría
   context AttackHarmDetection
   inv: self.SecurityRole→size()=1
   inv: self.mSecRole.mGAuReg→size()>=1
2. El nombre del rol de seguridad que se genera a partir de una especificación de detección de ataques y amenazas que se hizo sobre un almacén de datos o un flujo de objetos deberá ser el mismo nombre de la partición o región que los contiene.
   context AttackHarmDetection
   inv: if self.DataStoreNode→size()=1 then
   self.interruptibleRegion→size()>=1 implies
   self.mSRole.SecurityRoleName=self.interruptibleRegion.Name
   else
   self.inPartition→size>=1 implies
   self.mSRole.SecurityRoleName=self.inPartition.Name
   endif
   inv: if self.ObjectFlow→size()=1 then
   self.interrups→size()>=1 implies
   self.mSRole.SecurityRoleName=self.interrups.Name
   else
   self.inPartition→size>=1 implies
   self.mSRole.SecurityRoleName=self.inPartition.Name
   endif
3. Cuando exista una doble especificación de detección de ataques y amenazas, el rol de seguridad tomará el nombre de la partición o región que lo contenga
   context AttackHarmDetection
   inv: self.ActivityPartition→size()>1 and
   (self.Action→size()=1 or self.DataStoreNode→size()=1 or
   self.ObjectFlow→size()=1) implies
   self.mSRole.SecurityRoleName=self.mPartition.Name
   inv: self.InterruptibleActivityRegion→size()>1 and
   (self.Action→size()=1 or self.DataStoreNode→size()=1 or
   self.ObjectFlow→size()=1) implies
   self.mSRole.SecurityRoleName=self.mRegion.Name

Nombre: **AuditRegister**

Generalización: Element (from Kernel)

Descripción: Es un clase abstracta que contiene las especificaciones de registro de auditoría relacionadas con la especificación de requisitos de seguridad. Cada registro de auditoria debe ser especializado en una de sus subclases.

Asociaciones: No tiene

Notación:  Esta notación es una asociación entre el requisito de seguridad y el símbolo usado para hacer anotaciones o comentarios

Valores Etiquetados: No tiene

Restricciones: No tiene

Nombre: **G-AuditRegister**

Generalización: AuditRegister

Descripción: Contiene las especificaciones de registro de auditoría relacionadas con un rol de seguridad. Los requisitos de seguridad control de acceso, detección de ataques y amenazas, integridad y privacidad, que generan un rol de seguridad, se relacionan con G-AuditRegister.

Asociaciones: SecurityRole [1..1]

Notación: No tiene

Valores Etiquetados: AcDgElementName, AcDgElementType, AuditDate, AuditTime, SecurityRoleName, SourceSecReq

Restricciones:

1. La relación del requisito de seguridad con el rol deseguridad se determina por el valor de SourceSecReq. Los valores válidos son AC para control de acceso, AD para detección de ataques y amenazas, I para integridad y P para privacidad.
   context G-AuditRegister
   inv: self.mAccCon→size()=1 implies self.SourceSecReq="AC"
   inv: self.mAHDetec→size()=1 implies self.SourceSecReq="AD"
   inv: self.mIntegrity→size()=1 implies self.SourceSecReq="I"
   inv: self.mPrivacy→size()=1 implies self.SourceSecReq="P"

Nombre: **Integrity**

Generalización: SecurityRequirement

Descripción: La integridad está relacionada con la protección de componentes de corrupción intencional y no autorizada. La especificación de integridad esta graduada en baja, media y alta. Desde la perspectiva del analista de negocios una especificación de integridad (en cualquier grado) tiene relación con la importancia que tiene la información contenida en el almacén de datos. La especificación de integridad desde la perspectiva del experto en seguridad implica registrar el rol involucrado, fecha y hora de acceso al almacén. Adicionalmente se especifican medidas de seguridad de acuerdo con el grado de integridad. Este requisito siempre tiene asociado un registro de auditoría

Asociaciones: DataStoreNode [0..*], ObjectFlow [0..*],SecurityRole [1..1]

Notación: 

Valores Etiquetados: AcDgElementName, AcDgElementType, KindIntegrity

Restricciones

1. La integridad debe tener asociado un rol de seguridad y registro de auditoría
   context Integrity
   inv: self.SecurityRole→size()=1
   inv: and self.mSecRole.mGAuReg→size()>=1
2. El grado de protección debe ser agregado agregando una letra minúscula de acuerdo con los valores de KindIntegrity. La letra ***x*** debe ser reemplazada por **w** para bajo, **m** para medio o **h** para alto.
   context Integrity
   inv: self.KindIntegrity→size()=1

Nombre: **NonRepudiation**

Generalización: SecurityRequirement

Descripción: Establece la necesidad de evitar la denegación de cualquier aspecto de la interacción (por ejemplo, mensajes, transacciones, transmisión de datos).

Desde la perspectiva del analista de negocios, No repudio representa la necesidad de proteger una determinada interacción, de manera que minimice los potenciales problemas (e.g. legal y/o fiscal) en relación con alguna interacción. Desde la perspectiva de la seguridad esta especificación implica la generación de al menos dos roles de seguridad y alternativamente el registro de auditoría. Este requisito adicionalmente puede tener una especificación de registro de auditoría

Asociaciones: NR-AuditRegister [0..*] ObjectFlow [0..*], SecurityRole [2..*]

Notación: 

Valores Etiquetados: AcDgElementName, ActionDestinationName, AuditRegister, SecurityRoleDestinationName, SecurityRoleSourceName

Restricciones:

1. Se puede especificar registro de auditoría para No repudio
   context NonRepudiation
   inv: self.AuditRegister=True implies self.NR-AuditRegister→size()>=1
2. Está relacionado con a lo menos dos roles de seguridad, el que envía y el que recibe
   context NonRepudiation
   inv: self.SecurityRole→size()>=2

Nombre: **NR-AuditRegister**

Generalización: AuditRegister

Descripción: Contiene una especificación de auditoría relacionada con el requisito de seguridad No repudio.

Asociaciones: NonRepudiation [1..1]

Notación: No tiene

Valores Etiquetados: AcDgElementName, AuditDateReceive, AuditDateSend, AuditTimeReceive, AuditTimeSend, SecurityRoleDestinationName, SecurityRoleSourceName, Transmission

Restricciones

1. Es válido si se ha especificado un requisito de seguridad de No repudio
   context NR-AuditRegister
   inv: self.NonRepudiation→size()=1

Nombre: **Privacy**

Generalización: SecurityRequirement

Descripción: Está relacionada con condiciones de protección de la información acerca de un determinado individuo o entidad, limitando el acceso a partes no autorizadas a obtener información sensible. Desde el punto de vista del analista de negocios la especificación de privacidad implica la no revelación (confidencialidad) y no almacenaje (anonimato) de la información acerca de un determinado rol. Desde el punto de vista de la seguridad la especificación de privacidad con confidencialidad implica proteger la información acerca de un rol para que no sea develada a terceros. En caso de la privacidad con anonimato implica que la información además no debe ser almacenada. Esto último implica la creación de roles genéricos que expiran junto con la sesión de trabajo. Este requisito adicionalmente puede tener una especificación de registro de auditoría

Asociaciones: ActivityPartition [0..*], InterruptibleActivityRegion [0..*], SecurityRole[1..1]

Notación: 

Valores Etiquetados: AcDgElementName, AcDgElementType, AuditRegister, KindPrivacy

Restricciones:

1. Un requisito de Privacidad debe tener un rol de seguridad asociado
   context Privacy
   inv: self.SecurityRole→size()=1
2. El tipo de privacidad debe ser especificado con una letra minúscula de acuerdo con el valor de PrivacyType. La letra ***x*** debe ser reemplazada por **a** para anonimato o **c** para confidencialidad
   context Privacy
   inv: self.KindPrivacy–>size()=1
3. Cuando se especifica privacidad con auditoria se debe crear un estereotipo G-AuditRegister asociado al rol de seguridad
   context Privacy
   inv: self.AuditRegister=True implies self.G-AuditRegister→size()>=1

Nombre: **SecureActivity**

Generalización: Activity

Descripción: Es una clase abstracta que contiene las especificaciones relacionadas con requisitos, roles y permisos de seguridad

Asociaciones: SecurityRequirement [1..*]

Notación: No tiene

Valores Etiquetados: No tiene

Restricciones:

1. Debe estar asociada por lo menos con un requisito de seguridad
   context SecureActivity
   inv: self.SecurityRequirement→size()>=1

Nombre: **SecurityPermission**

Generalización: Element (from Kernel)

Descripción: Contiene las especificaciones de permisos relacionadas con especificaciones de control de acceso. Un permiso debe contener el nombre del objeto y las operaciones permitidas.

Asociaciones: SecureRole [1..1], SP-AuditRegister [0..*]

Notación: No tiene

Valores Etiquetados: AcDgElementName, AcDgElementType, KindPermission, SecurityRoleName, SourceSecReq

Restricciones

1. Un permiso de seguridad sólo existe si se ha especificado control de acceso.
   context SecurityPermission
   inv: self.mSecRole.SourceSecReq="AC" implies self.SecurityPermission→size()>=1
2. Puede tener especificación de registro de auditoría
   context SecurityPermission
   inv: self.mSecRole.mAccCon.AuditRegister=True implies self.SP-AuditRegister→size()>=1
3. Un tipo de permiso (KindPermission) debe ser especificado para las acciones, datos o flujos de objetos como un par objeto/operación.
   context SecurityPermissions
   inv: self.Actions–>size()=1 implies (self.KindPermission="Execution" or self.KindPermission="CheckExecution")
   inv: self.DatastoreNode–>size()=1 implies (self.KindPermission="Update" or self.KindPermission="Create" or self.KindPermission="Read" or self.KindPermission="Delete")
   inv: self.ObjectFlow–>size()=1 implies (self.KindPermission="SendReceive" or self.KindPermission="CheckSendReceive")

Nombre: **SecurityRequirement**

Generalización: Element (from Kernel)

Descripción: Clase abstracta que contiene las especificaciones de requisitos de seguridad. Cada requisito de seguridad debe ser indicado como una subclase.

Asociaciones: SecureActivity [1..1]

Notación:  Representa el símbolo básico sobre el cual se especifica un requisito de seguridad. Ha sido adoptado porque se considera un estándar *de facto* asociado al concepto de seguridad

Valores Etiquetados: No tiene

Restricciones:

1. La notación debe ser especializada con una de sus subclases. Un requisito de seguridad debe ser especificado

Nombre: **SecurityRole**

Generalización: Actor (from UseCases)

Descripción: Contiene la especificación de un rol de seguridad. Se relaciona con todos los requisitos de seguridad y con el registro genérico de auditoría.

*Asociaciones:*AccessControl [0..*], AttakHarmDetection[0..*], G-AuditRegister [0..*], Integrity[0..*], NonRepudiation [0..*], Privacy [0..*], SecurityPermission [0..*]

Notación: No tiene

Valores Etiquetados: AcDgElementName, AcDgElementType, KindPrivacy, SecurityRoleName, SourceSecReq

Restricciones:

1. Un rol de seguridad puede ser originado a partir de una especificación de un requisito de control de acceso, detección de ataques y amenazas, integridad, no repudio o privacidad, o como una combinación de esos requisitos. Las combinaciones válidas se encuentran definidas en el valor que puede tomar el tipo de dato RequirementType

Nombre: **SP-AuditRegister**

Generalización: AuditRegister

Descripción: Contiene las especificaciones de registro de auditoría relacionada con los permisos derivados de la especificación de control de acceso.

Asociaciones: SecurityPermission [1..1]

Notación: No tiene

Valores Etiquetados: AcDgElementName, AcDgElementType, AuditDate, AuditTime, KindPermission, SecurityRoleName

Restricciones

1. Una especificación de reigistro de auditoria de permisos existe sólo si se ha especificado control de acceso con auditoría.
   context SP-AuditRegister
   inv: self.SecPer.self.mSecRole.self.mAccCon.AudirRegister=True implies self.SP-AuditRegister→size()>=1

Para cada tipo de dato se especifica nombre, descripción, generalización (clase base), valores y los estereotipos que lo usan. Los tipos de datos se describen en la Tabla 2 en orden alfabético.

Tabla 2: Descripción de tipos de datos

Nombre: **PermissionOperation**
Descripción: Este estereotipo contiene los valores permitidos asociados con permisos de operación. Los valores se asocian a cada elemento que se encuentra en el ámbito de una especificación de control de acceso
Generalización: Classifier::DataType::Enumeration
Valores: {"Execution", "CheckExecution", "Create", "Delete", "Read", "Update", "SendReceive", "CheckSendReceive"}
- Actions {Execution, CheckExecution}
  - *Execution* (valor por defecto); La acción pueden ser ejecutada cuando una restricción de control de acceso ha sido especificada y *CheckExecution*: La acción puede ser ejecutada después de verificar el permiso de ejecución
- DataStoreNode {Create, Delete, Read, Update}
  - *Create, Delete, Read* and *Update* (valor por defecto)
- ObjectFlow {SendReceive, CheckSendRecieve}
  - *SendReceive* (valor por defecto); El flujo de objeto puede ser enviado o recibido cuando se ha especificado un requisito de control de acceso y *CheckSendRecieve*; el permiso derivado de la especificación de control de acceso debe ser verificado antes de enviar o recibir el flujo de objeto.

Usado por: SecurityPermission, SP-AuditRegister

Nombre: **PrivacyType**
Descripción: Contiene información acerca del tipo de privacidad. Es decir, anonimato o confidencialidad.
Generalización: Classifier::DataType::Enumeration
Valores: {"a", "c"}
Usado por: Privacy, SecurityRole

Nombre: **ProtectionDegree**
Descripción: Contiene una clasificación del grado de protección en relación con la integridad. Este valor puede ser bajo (w), medio (m) o alto (h).
Generalización: Classifier::DataType::Enumeration
Valores: {"w", "m", "h"}
Usado por: Integrity

Nombre: **RequirementType**:
Descripción: Contiene los valores posibles en relación con las combinaciones de requisitos de seguridad que pueden ser especificados. Se construye como una combinación de las abreviaturas AC, AD, I, NR y P asociadas a control de acceso, detección de ataque y amenazas, integridad, no repudio y privacidad respectivamente.
Generalización: Classifier::DataType::Enumeration
Valores: {"AC", "AD", "I", "NR","P", "ACAD", "ACP", "ADP", "ACADP" "ACI", "ADI", "ACADI", "ACNR", "ADNR", "INR", "ACADNR", "ADINR", "ACADINR"}
Usado por: G-AuditRegister, SecurityPermission, SecurityRole

5. Ejemplo

El proceso de negocio, relacionado con la admisión de pacientes en una institución médica, se inicia con una Solicitud de Atención que es rellenada por un Paciente. Este documento, es enviado al Área de Administración para capturar la información relacionada con los seguros médicos y verificar la existencia de una Ficha Clínica asociada al paciente. Una vez que se verifica que la documentación del paciente sea válida y este completa es enviada al Área Médica. El área de Evaluación Médica determina, a través de un conjunto de pruebas de pre-admisión, la condición médica del paciente. Si fuera necesario se harán exámenes adicionales que deberán ser registrados desde el punto de vista clínico y económico. Finalmente se completa el documento Evaluación Médica con información acerca del paciente, el cual se le envía. El proceso de negocio termina cuando el paciente ha recibido la Evaluación Médica.

La construcción del proceso de negocio es realizada en una primera instancia por el analista de negocios. Al mismo tiempo agrega los requisitos de seguridad que posteriormente son refinados en compañía del experto en seguridad. El resultado final de esta tarea se muestra en la Figura 7.

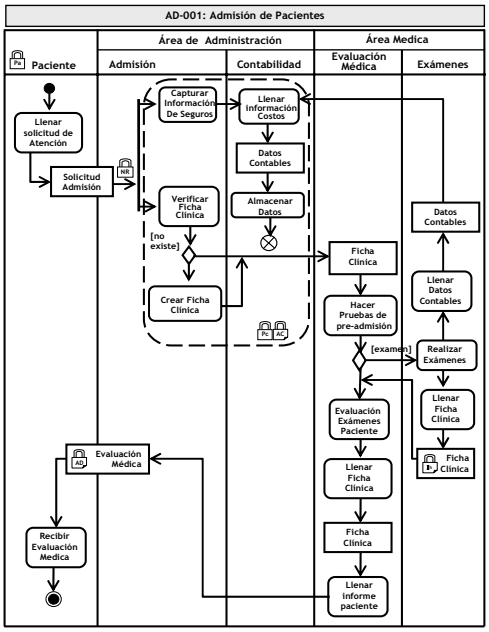

Figura 7 Admisión de Pacientes

Se han identificado siete particiones (*Activity Partition*), una región (*Interruptible Activity Region*), siete almacenes de datos (*Data Store Node*) y trece acciones (*Actions*). Junto con ello se ha identificado privacidad (con anonimato) para la partición Paciente, con el propósito de prevenir la obtención y almacenaje de información sensible acerca del paciente. Se ha especificado no repudio sobre el flujo de datos "Solicitud Admisión" con la intención de evitar la negación de la recepción del documento. Los requisitos de seguridad

control de acceso con registro de auditoría y privacidad con confidencialidad han sido especificados sobre la región que se encuentra entre las particiones Admisión y Contabilidad (ver permisos en Tabla 3). También se ha especificado integridad (alta) sobre el almacén de datos "Ficha Clínica" con la intención de proteger de manera especial ese documento. Finalmente, se ha especificado detección de ataques y amenazas sobre el almacén de datos "Evaluación Médica" con la idea de registrar todos los eventos relacionados con intentos, fallidos y exitosos, de ataques o daños que se hagan sobre el documento.

Tabla 3: Permisos relacionados con el control de acceso

Elemento de UML 2.0-AD		
Nombre	Tipo	Permiso
Capturar información de seguros	Action	Execution
Llenar información de costos	Action	CheckExecution
Verificar Ficha Clínica	Action	Execution
Almacenar Datos	Action	Execution
Crear Ficha Clínica	Action	Execution
Datos contables	DataStoreNode	Update

6. Conclusiones y trabajo futuro

En la última versión de UML se ha cambiado el diagrama de actividad permitiendo una mejor la representación de procesos de negocio. Para los expertos del negocio esto implica contar con un nuevo lenguaje para representar sus procesos. Para los desarrolladores de software es una oportunidad para identificar requisitos, puesto que la descripción del proceso de negocio será utilizada en conjunto con las técnicas ya existentes para la captura de requisitos.

Por su parte, la seguridad se ha convertido en un aspecto de mucha importancia para el desempeño del negocio. Sin embargo, no ha sido considerada en UML 2.0-AD. En este artículo hemos presentado una extensión de UML 2.0-AD que permite incorporar requisitos de seguridad en la descripción de un proceso de negocio. Con esto se agrega una perspectiva adicional en el ámbito de los procesos de negocio que además repercutirá favorablemente en la identificación de requisitos en el contexto del desarrollo de sistemas.

Los siguientes pasos en esta investigación están orientados a enriquecer la especificación de la extensión incorporando reglas de buena formación, a mejorar la herramienta que permite diseñar procesos de negocio seguros y a construir casos reales que permitan retroalimentar esta propuesta.

Agradecimientos

Esta investigación es parte de los proyectos DIMENSIONS (PBC-05-012-1) y MISTICO (PBC06-0082), ambos parcialmente financiado por el FEDER y por la Consejería de Educación y Ciencia de la Junta de Comunidades de Castilla-La Mancha, España; COMPETISOFT (506AC287) concedido por CYTED y ESFINGE (TIN2006-15175-C05-05/) otorgado por la Dirección General de Investigación del Ministerio de Ciencia y Tecnología, España.

Referencias

[1] Atluri, V. Security for Workflow Systems, Information Security Technical Report, Vol. 6 (2), (2001), pp. 59-68.

[2] Backes, M., Pfitzmann, B., y Waider, M. Security in Business Process Engineering, International Conference on Business Process Management (BPM), Eindhoven, Netherlands., (2003), pp. 168-183.

[3] BPMN. Business Process Modeling Notation Specification: OMG Final Adopted Specification, dtc/06-02-01, 2006.

[4] Eriksson, H.-E. y Penker, M. Business Modeling with UML, OMG Press, (2001) p.

[5] Firesmith, D. Engineering Security Requirements, Journal of Object Technology, Vol. 2 (1), January-February, (2003), pp. 53-68.

[6] Firesmith, D. Specifying Reusable Security Requirements, Journal of Object Technology, Vol. 3 (1), January-February., (2004), pp. 61-75.

[7] Haley, C. B., Laney, R. C., y Nuseibeh, B. Deriving security requirements from crosscutting threat descriptions, 3rd International Conference on Aspect-Oriented Software Development (AOSD), Lancaster, UK, (2004), pp. 112-121.

[8] Harmon, P. The OMG's Model Driven Architecture and BPM, 2005: .Business Process Trends, Vol. 2 (5), 2004.

[9] Herrmann, G. y Pernul, G. Viewing Business Process Security from Different Perspectives, 11th International Bled Electronic Commerce Conference, Slovenia., (1998), pp. 89-103.

[10] Herrmann, P. y Herrmann, G. Security requirement analysis of business processes, Electronic Commerce Research, Vol. 6 (3-4), (2006), pp. 305-335.
[11] Jacobson, I., Booch, G., y Rumbaugh, J. The Unified Software Development Process, (1999) 463 p.
[12] Kalnins, A., Barzdins, J., y Celms, E. UML Business Modeling Profile, Thirteenth International Conference on Information Systems Development, Advances in Theory, Practice and Education, Vilnius, Lithuania, (2004), pp. 182-194.
[13] Korherr, B. y List, B. Extending the UML 2 Activity Diagram with Business Process Goals and Performance Measures and the Mapping to BPEL, 2nd International Workshop on Best Practices of UML (BP-UML) at ER Conference, Tucson, Arizona, USA, (2006), pp. 7-18.
[14] Lampson, B. W. Computer Security in the Real World, IEEE Computer, Vol. 37 (6), (2004), pp. 37-46.
[15] List, B. y Korherr, B. A UML 2 Profile for Business Process Modelling, 1st International Workshop on Best Practices of UML (BP-UML) at ER-Conference, Klagenfurt, Austria, (2005).
[16] Lonjon, A. Business Process Modeling and Standardization, BPTrends, In http://www.bptrends.com/, (2004).
[17] Maña, A., Montenegro, J. A., Rudolph, C., y Vivas, J. L. A business process-driven approach to security engineering, 14th. International Workshop on Database and Expert Systems Applications (DEXA). Prague, Czech Republic., (2003), pp. 477-481.
[18] Object Management Group. MDA Guide Version 1.0.1, 2003.
[19] Object Management Group. Unified Modeling Language: Superstructure: version 2.0, formal/05-07-04, 2005.
[20] Object Management Group. OCL 2.0 Specification, Version 2.0, 2005.
[21] Object Management Group. Unified Modeling Language: Superstructure Version 2.1.1 (formal/2007-02-05), 2007.
[22] Podeswa, H. B.O.O.M.: Business Object-Oriented Modeling for Business Analysts, (2005) 401 p.
[23] Rational Software. Rational Unified Process, Best Practices for Software Development Teams, (2001) 21 p.
[24] Rodríguez, A., Fernández-Medina, E., y Piattini, M. Hacia la definición de un perfil de UML 2.0 para modelar requisitos de seguridad en procesos de negocio, XI Jornadas de Ingeniería del Software y Bases de Datos, Sitges, España, (2006), pp. 347-356.
[25] Röhm, A. W., Herrmann, G., y Pernul, G. A Language for Modelling Secure Business Transactions, 15th. Annual Computer Security Applications Conference., Phoenix, Arizona., (1999), pp. 22-31.
[26] Stefanov, V., List, B., y Korherr, B. Extending UML 2 Activity Diagrams with Business Intelligence Objects, 7th International Conference on Data Warehousing and Knowledge Discovery (DaWaK2005), Copenhagen, Denmark, (2005).
[27] Vitolins, V. y Kalnins, A. Semantics of UML 2.0 Activity Diagram for Business Modeling by Means of Virtual Machine, Ninth IEEE International Enterprise Distributed Object Computing Conference (EDOC), Enschede, The Netherlands, (2005), pp. 181-194.
[28] Vivas, J. L., Montenegro, J. A., y Lopez, J. Towards a Business Process-Driven Framework for security Engineering with the UML, Information Security: 6th International Conference, ISC, Bristol, U.K., (2003), pp. 381-395.