Actas de la IX Reunión Española sobre Criptología y Seguridad de la Información

Casa de Convalescència, Hospital de la Santa Creu i Sant Pau

7, 8 y 9 de septiembre del 2006, Barcelona

Departament d'Enginyeria de la Informació i les Comunicacions,
Universitat Autònoma de Barcelona
Estudis d'Informàtica, Multimèdia i Telecomunicacions,
Universitat Oberta de Catalunya

Editores
Joan Borrell Viader
Jordi Herrera Joancomartí

Editores: Joan Borrell Viader y Jordi Herrera Joancomartí.

Primera edición: julio 2006.
ISBN: 84-9788-502-3

Prólogo

Esta publicación recoge las actas de la Reunión Española sobre Criptología y Seguridad de la Información (RECSI), celebrada los días 7, 8 y 9 de septiembre del 2006 en Barcelona.

La RECSI llega en el año 2006 a su novena edición, organizada de forma conjunta por el Departamento de Ingeniería de la Información y de las Comunicaciones de la Universidad Autònoma de Barcelona y el Departamento de Informática y Multimedia de la Universidad Oberta de Catalunya. Esta IX RECSI quiere seguir siendo el lugar de encuentro y el foro en el que los criptólogos y, en general, todos aquellos que trabajan en el campo de la Seguridad de la Información expongan sus hallazgos y debatan sus ideas. Se trata de un congreso bienal que se celebra en universidades y centros de investigación de España. Las ediciones anteriores se llevaron a cabo en Palma de Mallorca (U. Illes Balears), Madrid (CSIC), Barcelona (U. Politècnica de Catalunya), Valladolid (U. de Valladolid), Torremolinos (U. de Málaga), Santa Cruz de Tenerife (U. de La Laguna), Oviedo (U. de Oviedo) y Leganés (U. Carlos III).

La expansión de Internet, el incremento exponencial del volumen de datos automatizados que se maneja, la creciente inquietud por la protección de la intimidad y, en general, la entrada en la era de la información hace que la seguridad de ésta se configure como un campo de singular importancia, y por ello concentre un especial interés por parte de las empresas, las administraciones, los profesionales y más ampliamente, la sociedad entera. Por otro lado, la Criptología, en su doble vertiente de diseño de algoritmos criptográficos y de análisis de sus posibles debilidades, se ha convertido en la disciplina vertebral de la seguridad, habiendo abandonado los círculos impenetrables en los que se desplegaba históricamente, para ser tratada en universidades, centros de investigación, empresas y organismos de todo tipo interesados en proteger las informaciones que manejan.

Conscientes de lo anterior, en la IX RECSI se tratan y profundizan los aspectos de estas materias que más despiertan la atención en estos días, así como otros, aún en investigación, pero que están llamados a ser de capital importancia en los sistemas y mecanismos de seguridad en un inmediato futuro. A lo largo de las tres jornadas que conforman la Reunión se presentan 63 comunicaciones en 18 sesiones paralelas. Queremos agradecer desde estas líneas el trabajo realizado por el Comité Científico y los revisores en el proceso de revisión.

La IX RECSI, buscando mantener un elevado nivel académico y también un adecuado nivel de contacto de la comunidad investigadora con las empresas y la sociedad, incluye también:

- Tres conferencias magistrales a cargo de investigadores de reconocido prestigio en el ámbito de la Criptología y la Seguridad de la Información, el Dr. Moni Naor, del Weizmann Institute of Science (Israel), el Dr. Frédéric Cuppens de la Escuela Normal Superior de Telecomunicaciones de Bretaña

(Francia) y el Dr. Gene Tsudik de la Universidad de California en Irvine (USA).

- Dos presentaciones de empresas, Safelayer Secure Communications, compañía líder en el mercado de seguridad y confianza para las TIC, desarrollando tecnología de identificación electrónica, firma electrónica y protección de datos basada en Infraestructura de Clave Pública (PKI), y Scytl Secure Electronic Voting, compañía líder en el desarrollo de plataformas de votación electrónica seguras y confiables, aplicables desde procesos electorales clásicos a juntas generales de accionistas.
- La presentación de la Unidad Central de Informática Forense de la Policía de la Generalitat de Catalunya - Mossos d'Esquadra.

Manifestar también nuestro agradecimiento por la ayuda financiera y de difusión recibida de los distintos patrocinadores, cuya relación aparece en la página de agradecimientos de estas actas.

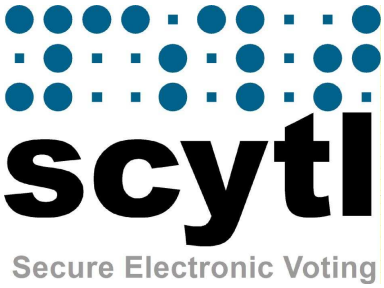
No quisieramos finalizar este prólogo sin recordar a nuestro amigo Andreu Riera Jorba, participante en varias Reuniones, tristemente fallecido en accidente de coche el 11 de marzo de 2006. Andreu, doctor por la UAB, era conocido tanto por su valiosa aportación en el campo de la criptografía aplicada al voto electrónico, como por su espíritu emprendedor que le llevó a fundar Scytl Secure Electronic Voting, empresa de la cual era Consejero Delegado.

Septiembre 2006

Joan Borrell Viader
Jordi Herrera Joancomartí

Agradecimientos

Los organizadores de la RECSI quieren agradecer a los patrocinadores de la Reunión su apoyo logístico y económico.



Organización

La IX RECSI ha sido organizada conjuntamente por el Departament d'Enginyeria de la Informació i les Comunicacions de la Universitat Autònoma de Barcelona y los Estudis d'Informàtica, Multimèdia i Telecomunicacions de la Universitat Oberta de Catalunya.

Comité ejecutivo

Joan Borrell Viader
Jordi Herrera Joancomartí
Josep Rifà Coma

Comité científico

Abascal Fuentes, Policarpo (U. de Oviedo)
Arranz Chacón, Maria Luisa (Alcatel)
Areitio Bertolín, Javier (U. de Deusto)
Borrell Viader, Joan (U.Autònoma de Barcelona)
Caballero Gil, Pino (U. de La Laguna)
Dávila Muro, Jorge (U. Politécnica de Madrid)
Domingo-Ferrer, Josep (U. Rovira i Virgili)
Fernández-Medina Patón, Eduardo (U. de Castilla La Mancha)
Ferrer Gomila, Josep Lluis (U. de les Illes Balears)
Fúster Sabater, Amparo (CSIC)
Gómez Skarmeta, Antonio (U. de Múrcia)
González Jiménez, Santos (U. de Oviedo)
Guía Martínez, Dolores de la (CSIC)
Gutiérrez Gutiérrez, Jaime (U. de Cantabria)
Herrera Joancomartí, Jordi (U. Oberta de Catalunya)
Huguet Rotger, Llorenç (U. de les Illes Balears)
López Muñoz, Javier (U. de Málaga)
Martín del Rey, Angel (U. de Salamanca)
Mañas Argemí, José Antonio (U. Politécnica de Madrid)
Miret Biosca, Josep Maria (U. de Lleida)
Padró Laimon, Carles (U. Politècnica de Catalunya)
Peinado Domínguez, Alberto (U. de Málaga)
Ramió Aguirre, Jorge (U. Politécnica de Madrid)
Ramos Álvarez, Benjamín (U. Carlos III de Madrid)
Ribagorda Garnacho, Arturo (U. Carlos III de Madrid)
Rifà Coma, Josep (U. Autónoma de Barcelona)
Robles Martínez, Sergi (U. Autónoma de Barcelona)

Salazar Riaño, Jose Luís (U. de Zaragoza)
Sempere Luna, José Maria (U. Politécnica de Valencia)
Soriano Ibáñez, Miquel (U. Politècnica de Catalunya)
Rifà Coma, Josep (U. Autònoma de Barcelona)
Tena Ayuso, Juan (U. de Valladolid)
Villar Santos, Jorge (U. Politècnica de Catalunya)

Comité Organizador

Joan Arnedo (Universitat Oberta de Catalunya)
Carles Garrigues (Universitat Autònoma de Barcelona)
David Megías (Universitat Oberta de Catalunya)
Alvaro Moratalla (Universitat Autònoma de Barcelona)
Guillermo Navarro (Universitat Autònoma de Barcelona)
Josep Prieto (Universitat Oberta de Catalunya)
Segi Robles (Universitat Autònoma de Barcelona)
Jordi Serra (Universitat Oberta de Catalunya)
Pere Urbón (Universitat Autònoma de Barcelona)

Revisores

Guillermo Azuara Guillén
Óscar Cánovas Reverte
Jordi Castellà Roca
Sergio Castillo Pérez
Vanesa Daza Fernández
Oscar Esparza Martín
Juan M. Estévez Tapiador
Joaquín García Alfaro
Félix J. García Clemente
Maria Isabel González Vasco
Julio César Hernández Castro
Gabriel López Millán
Consuelo Martínez López
Antoni Martínez Ballesté
Gregorio Martinez Perez
José Luis Muñoz-Tapia
Josep Pegueroles
Joan Josep Piles Contreras
Helena Rifà Pous
Francesc Sebé Feixas
Agusti Solanas Gómez

Índice general

Sesión C1

Sesión S1

Sesión C2

Sesión S2

Sesión C3

Sesión S3

Sesión C4

Sesión S4

Sesión C5

Sesión S5

Sesión S6

Sesión S7

Sesión C6

Sesión S8

Sesión S12

Extensión de Diagramas de Actividad de UML 2.0 para el Modelado de RBAC

Alfonso Rodríguez[1], Eduardo Fernández-Medina[2], and Mario Piattini[2]

[1] Departamento de Auditoría e Informática,
Universidad del Bio Bio,
La Castilla S/N, Chillán, Chile.
alfonso@ubiobio.cl.
[2] Grupo ALARCOS
Departamento de Tecnologías y Sistemas de Información
Centro Mixto de Investigación y Desarrollo de Software UCLM-Soluziona
Universidad de Castilla-La Mancha
Paseo de la Universidad 4 - 13071, Ciudad Real, España.
Eduardo.FdezMedina, Mario.Piattini@uclm.es

Resumen Los procesos de negocio son esenciales para muchas empresas porque les permiten mantener su competitividad. También son importantes para los desarrolladores de software porque es posible obtener desde allí los requisitos necesarios para el diseño y la construcción de sistemas de información. Por su parte, la seguridad es un tema de especial relevancia, aunque tradicionalmente sea considerada después de la definición del proceso de negocio. Esto sucede a pesar de la existencia de estudios empíricos que muestran que consumidores, usuarios finales y analistas de negocios son capaces de expresar sus necesidades de seguridad. En este artículo presentamos una extensión de los diagramas de actividad de UML 2.0 que permite identificar roles y permisos orientados a implementar una política de control de acceso basado en roles. Complementamos nuestra propuesta con un ejemplo ilustrativo acerca de un proceso de negocio para la atención de pacientes en una institución de salud.

1. Introducción

La clave para mantener la competitividad en las empresas está estrechamente vinculada con la capacidad que ellas tengan para describir, estandarizar y adaptar la forma en que interactúan con sus proveedores, socios, competidores y clientes [30]. Los Procesos de Negocio, definidos como un conjunto de procedimientos o actividades que llevan a cabo, colectivamente, los objetivos o políticas del negocio [37], han resultado ser una buena respuesta ante la complejidad del entorno, la velocidad con que se requieren los nuevos productos y el creciente número y variedad de actores involucrados en las actividades cotidianas de las organizaciones. Por su parte, el nuevo escenario en que se desarrollan los negocios, con la introducción del comercio electrónico y el uso intensivo de comunicaciones y tecnologías de información, propicia que las empresas junto con ampliar sus

negocios, también aumenten su vulnerabilidad. La consecuencia más inmediata es que, dado el creciente número de ataques sobre los sistemas, es altamente probable que tarde o temprano algún intruso tenga éxito [27]. Esta violación de la seguridad causa pérdidas en las organizaciones, razón por la cual es necesario proteger sus computadores y sus sistemas de la mejor forma posible. Esto no significa seguridad absoluta, sino un razonable alto nivel de seguridad en relación a las limitaciones que se tienen [38].

Aunque se reconoce la importancia de la seguridad, ésta ha sido a menudo descuidada en el modelado de procesos de negocio, ya que generalmente se concentran en el modelado del proceso propiamente dicho [3]. Esto se debe a que el experto en el dominio del proceso de negocio no es un especialista en seguridad [16]. Usualmente la seguridad es considerada después de la definición del sistema. Este enfoque a menudo ocasiona problemas con la consecuente pérdida de tiempo y se transforma, en forma posterior, en vulnerabilidades de seguridad [24]. Tampoco los ingenieros de requisitos están entrenados del todo en seguridad y los pocos que han sido 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 [13].

Si se considera que la especificación de requisitos da lugar, generalmente, a una especificación del software que tendrá que ser tan exacta como sea posible [1], es posible concluir que una especificación temprana de las características de la seguridad de un proceso de negocio resulta positiva para el desarrollo de sistemas seguros. Por otra parte, la incorporación tardía de la seguridad aumenta la posibilidad de que exista un conflicto de seguridad en forma posterior y además aumenta el costo requerido para tratar de corregir la vulnerabilidad [24].

Por su parte, el control de acceso es uno de los requisitos de seguridad importantes para el buen funcionamiento de los sistemas de información. En particular, el control de acceso basado en roles (RBAC, Rol-Based Access Control) [4, 12, 32] ha resultado ser una solución muy atractiva para proveer características de seguridad en la administración de infraestructuras digitales multi-dominio. RBAC se caracteriza por la noción de permisos que son asignados a roles y no directamente a usuarios. De esta forma, los usuarios son asignados al rol más apropiado, de acuerdo con las funciones que desempeñan en su trabajo. Los usuarios adquieren indirectamente los permisos asociados a esos roles [19]. Ya que los roles representan funciones en la organización, el mecanismo de RBAC, puede soportar en forma directa las políticas de control de acceso definidas en una organización [4].

A su vez, los procesos de negocio que han sido bien modelados facilitan la discusiones entre los diferentes interesados, permitiéndoles ponerse de acuerdo sobre aspectos claves y trabajar en conjunto hacia las metas comunes. De manera que, resulta fundamental para la creación de software de calidad, contar con modelos de negocios que puedan ser entendidos y sometidos a mejoras [11].

Para el modelado de procesos de negocio existen diversos lenguajes y notaciones [15]. No obstante, BPMN (Business Process Modeling Notation) y UML (Unified Modeling Language) son considerados los principales estándares [23].

El cambio más importante de UML 2.0 respecto de sus versiones previas ha sido sobre los diagramas de actividad que han mejorado la representación de procesos de negocio. Nuestro trabajo considera una extensión de UML 2.0 para permitir la incorporación de requisitos de seguridad en los diagramas de actividad teniendo en cuenta la perspectiva del analista de negocios. Así, el analista de negocios podrá

identificar y representar algunos de los requisitos de seguridad propuestos en [14]. En particular, la especificación de control de acceso, dará origen a la identificación de roles y permisos que estarán asociados a elementos del diagrama de actividad usados para describir un determinado proceso de negocio.

La identificación temprana de requisitos de seguridad, usando notaciones ampliamente aceptadas como UML, permite implementar especificaciones independientes de la implementación, lo que permite la utilización del estándar MOF (Meta Object Facility) y la definición de arquitecturas dirigidas por modelos (MDA, Model Driven Architecture). De esta forma, un sistema puede ser modelado por niveles de abstracción o considerando diferentes perspectivas [20].

El resto del artículo se encuentra organizado como sigue: en la Sección 2 hemos resumido los principales antecedentes y los trabajos relacionados. En la Sección 3 proponemos una extensión que permite representar requisitos de seguridad desde la perspectiva del analista de negocios, considerando además, una identificación de roles y permisos orientados a la implementación del enfoque de control de acceso basado en roles. Finalmente, en la Sección 4, presentamos un ejemplo que nos permite ilustrar nuestra propuesta y en la Sección 5 presentamos nuestras conclusiones.

2 Antecedentes y trabajos relacionados

En esta sección resumiremos los principales tópicos relacionados con seguridad en procesos de negocio, control de acceso basado en roles, y diagramas de actividad y extensiones en UML 2.0. Los trabajos relacionados se han considerado en cada sub-sección.

2.1 Seguridad en procesos de negocio

A pesar de la importancia que supone la seguridad para los procesos de negocio, hemos podido detectar dos problemas: el primero de ellos está relacionado con el modelado propiamente dicho, el cual ha sido inadecuado, ya que generalmente quienes especifican los requisitos de seguridad son ingenieros de requisitos que han tendido, accidentalmente, a reemplazarlos por restricciones específicas de arquitectura [13]. Y en segundo lugar, y lo que en la práctica ha resultado ser lo más común, la seguridad ha sido integrada en forma tardía, a menudo durante la implementación real del proceso de manera ad-hoc [3], durante la fase de administración del sistema [20] o simplemente considerada como un servicio externo que será suministrado por un tercero [22]. Esto se explica, en parte, porque, a pesar de ser la seguridad un aspecto transversal que afecta tempranamente a los componentes de una aplicación, no es bien entendida y además hay carencia de herramientas que soporten la ingeniería de seguridad [20].

Una manera de modelar la seguridad que considera diversas perspectivas es la que se presenta en [16]. Los autores consideran las perspectivas: *estática*, sobre la seguridad de la información procesada, *funcional*, sobre los procesos del sistema, *dinámica*, sobre los requisitos de seguridad desde el ciclo de vida de los objetos involucrados en el proceso de negocio, *organizacional*, usada para relacionar las responsabilidades de los actores

con los procesos de negocio y de *procesos de negocio*, la que corresponde a una visión integrada de todas las perspectivas con un alto grado de abstracción. Nosotros creemos que en la perspectiva relacionada con los procesos de negocio, los analistas de negocios, pueden integrar su visión acerca de la seguridad en los negocios.

En cuanto a los requisitos, si bien los requisitos funcionales de seguridad tienden a variar entre aplicaciones de diverso tipo, no se puede decir lo mismo de los requisitos de seguridad, ya que cualquier aplicación en un alto nivel de abstracción tendrá la misma clase de valoración y potencialmente vulnerabilidad de sus activos [14]. De manera que, es posible establecer que los requisitos de seguridad que se pueden especificar en un proceso de negocio, sean del mismo tipo para todas las organizaciones, debido a que en este nivel no se está pensando en la implementación.

Los trabajos que se relacionan con especificaciones de seguridad por parte de los expertos en el dominio del negocio son; *(i)* pocos [3, 16, 21], *(ii)* se orientan a la seguridad en la transacción [29], *(iii)* apuntan directamente a los sistemas de información en general [35] o *(iv)* están pensados para ingenieros de seguridad e ingenieros de software [22]. Además, y considerando el vínculo existente entre procesos de negocio y flujos de trabajo (workflows) [36], hemos puesto especial atención en los trabajos que relacionan seguridad y workflow [2, 8]. Hemos podido comprobar que la mayoría de ellos pone énfasis en el control de acceso basado en roles [5, 8, 31].

2.2 Control de Acceso Basado en Roles (RBAC)

El modelo de referencia de RBAC (ver Figura 1) define tanto los términos que lo componen, usuarios, roles, permisos, operaciones y objetos, como las funciones y relaciones que se incluyen en este estándar. El concepto básico es que los usuarios y los permisos son asignados a roles. De esta forma, los usuarios tendrán permisos mientras estén desempeñado un determinado rol. Un rol es una función de trabajo o el título de un trabajo en una organización que describe la autoridad y responsabilidad de un usuario asignado a un determinado rol. Un permiso es un derecho concedido a un individuo que actúa sobre un determinado nombre de usuario asignado a un rol, que le permite al poseedor de los derechos actuar en el sistema dentro de los límites establecidos por esos derechos [1].

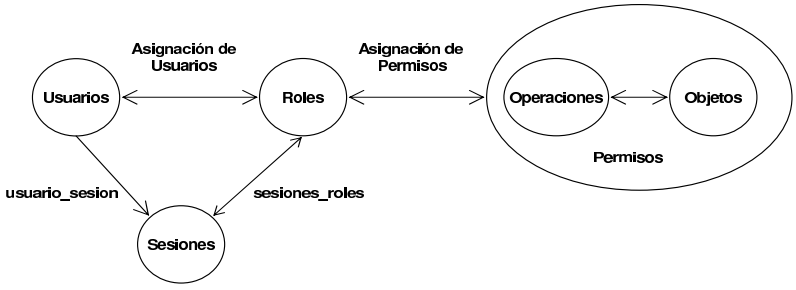


Fig. 1: Modelo de referencia de RBAC [12]

Existen varias razones para que RBAC sea bien aceptado como base para el modelo de control de acceso. Una de ellas es que el concepto de permisos basados en roles está estrechamente relacionado con el vocabulario del dominio usado para definir seguridad en las organizaciones. Esto permitiría facilitar la expresión de requisitos relevantes para el control de acceso durante la etapa de análisis así como promover su implementación en la etapa de diseño [20].

Trabajos relacionados con el control de acceso basado en roles y el modelado de proceso de negocio son presentados en [9] y [10]. Los autores muestran los conceptos básicos para construir un modelo de procesos de negocio basado en roles. El enfoque propuesto presenta dos modelos distintos: el modelo de objetos del negocio y el modelo de roles. El primer modelo se centra en la descripción de los objetos del negocio. Se representa el tipo de cada objeto del negocio, el comportamiento intrínseco y sus propiedades, pero no se representa las características de las relaciones de colaboración. Por su parte, en el modelo de roles, éstos son especificados como tipos que pueden ser especializados y agregados. La reutilización del rol es posible siempre que la semántica del patrón de interacción sea la misma. El modelo de roles describe el comportamiento de colaboración entre roles y las restricciones que lo regulan. Los roles están limitados a los objetos del negocio identificados en un modelo de objetos de negocio en que se define su contexto de uso.

En nuestra propuesta, la especificación de los requisitos de seguridad relacionados con el control de acceso, usando la extensión propuesta, es la base para hacer la especificación de RBAC.

2.3 Diagramas de actividad y extensiones en UML 2.0

Uno de los cambios más importante en la nueva versión de UML se ha producido en los diagramas de actividad [34]. En las versiones previas a UML 2.0, en relación al modelado de actividades, se había restringido la expresividad y confundido a los usuarios que no utilizan la orientación a objetos como enfoque para el modelado. Esta deficiencia de las versiones de UML 1.x ha sido considerada en la nueva versión de manera que es posible soportar el modelado de flujos a través de una amplia variedad de dominios [6]. Las actividades han sido rediseñadas para usar una semántica como la de las redes de Petri en vez de la semántica de las máquinas de estado. Entre otros beneficios esto amplía el número de flujos que pueden ser modelados, especialmente los que tienen flujos paralelos [25].

UML 2.0 se divide en especificaciones estructurales y de comportamiento, lo que permite el modelado de los aspectos estáticos y dinámicos de un sistema. Los modelos de comportamiento especifican cómo los aspectos estructurales de un sistema cambian en el tiempo. UML tiene tres modelos de comportamiento: actividades, máquinas de estado e interacciones. Las actividades se enfocan a representar secuencias, condiciones y entradas y salidas para invocar otros comportamientos, las máquinas de estado muestran cómo los eventos causan cambios en los estados de objetos e invocan otros comportamientos y los modelos de interacción describen los mensajes que pasan entre objetos que causan la invocación de otros comportamientos [7].

Los diagramas de actividad son los elementos de UML 2.0 que se usan para representar procesos de negocio y flujos de trabajos (workflows) [17, 26]. Para ello, el

modelamiento de las actividades pone énfasis en la secuencia y en las condiciones para la coordinación del comportamiento de bajo nivel tanto como de la propia clasificación de esos comportamientos. Esos son comúnmente llamados modelos de flujos de control y flujos de objetos. Una actividad especifica la coordinación de ejecución de una secuencia de unidades subordinadas cuyos elementos individuales son acciones. Cada acción puede ser ejecutada cero, una o más veces en cada ejecución de la actividad. Las acciones pueden ser ocurrencias de funciones primitivas, invocaciones a comportamiento, acciones de comunicación o manipulación de objetos [25].

La notación gráfica de una actividad, aunque opcional ya que puede ser reemplazada por una notación textual [25], es una combinación de nodos y conectores que permiten formar un flujo completo. Se consideran específicamente nodos de acción, control y objetos. Estos nodos son conectados por flujos de control y de objeto [6].

Por su parte, las extensiones en UML 2.0 se hacen utilizando perfiles. Este mecanismo permite extender los metamodelos existentes para adaptarlos con diferentes propósitos. Ello incluye la capacidad de ajustar el metamodelo a diferentes plataformas (por ejemplo: J2EE o .NET) o a distintos dominios (por ejemplo: tiempo real o modelado de proceso de negocio). Este mecanismo es consistente con Meta Object Facility de OMG [25].

Un Perfil está compuesto por estereotipos, restricciones y valores etiquetados. El *estereotipo* es un elemento del modelo definido mediante su nombre y la clase base a la que pertenece, la cual, normalmente es una meta-clase de UML. Las *restricciones* se aplican al estereotipo con el objeto de indicar limitaciones. Por ejemplo, expresar pre-condiciones, post-condiciones o invariantes. Las restricciones se pueden expresar en lenguaje natural, de programación o a través de OCL (Object Constraint Language). Los *valores etiquetados* son meta-atributos adicionales que se asignan al estereotipo y son especificados como el par nombre-valor.

Los trabajos relacionados con extensiones de UML 2.0 y procesos de negocio están referidos a características propias del negocio, tales como; metas, clientes, tipos de procesos de negocio y productos o servicios [18], almacenes de datos (data warehouse) y su relación con las estructuras dinámicas de los procesos de negocio, indicando dónde y cómo los procesos de negocio usan un entorno de almacenes de datos [33] o agregan semántica a las actividades considerando aspectos organizaciones que permitan expresar ciertas restricciones de recursos cuando se lleva a cabo una actividad [17]. Todos ellos extienden UML con perfiles agregando estereotipos al metamodelo.

3 Extensión de diagramas de actividad de UML 2.0 para el modelado de RBAC

Nuestro propósito es permitir que los analistas de negocios puedan especificar requisitos de seguridad en un proceso de negocio descrito mediante diagramas de actividad de UML 2.0. A partir de la especificación del requisito de seguridad Control de Acceso, se obtendrá una identificación de roles y permisos tendientes a especificar RBAC. Más tarde, los expertos en seguridad, transformarán esos requisitos de seguridad en especificaciones técnicas que incluyan los detalles necesarios para su implementación. En este trabajo hemos considerado sólo la primera parte.

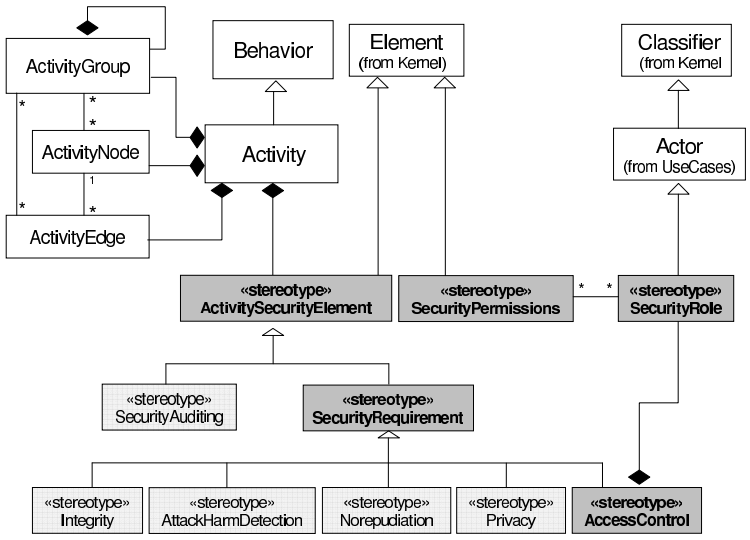


Fig. 2: Estereotipos para requisitos de seguridad e identificación de roles.

Nombre	**ActivitySecurityElement**	
Clase Base	Element (from Kernel)	
Descripción	Clase abstracta que contiene especificaciones de auditoría y requisitos de seguridad	
Nombre	**SecurityRequirement**	**Notación**
Clase Base	ActivitySecurityElement	
Descripción	Esta clase contiene una especificación de un requisito de seguridad**.** Debe especializarse para indicar el tipo de requisito	
Restricciones	Debe indicarse uno de los siguientes requisitos: (I) Integridad, (AC) Control de Acceso, (NR) No Repudio, (P) Privacidad y/o (AD) Detección de Amenazas y Ataques**.**	
Nombre	**AccessControl**	**Notación**
Clase Base	SecurityRequirement	
Descripción	Establece la necesidad de definir y/o intensificar los mecanismos de control de acceso para restringir el acceso a un determinado componente de un diagrama de actividad**.**	
Restricciones	Puede ser especificado sólo para los siguientes elementos del diagrama de actividad: Actividades (Activity), Particiones (ActivityPartition) y Regiones (InterruptibleActivityRegion)	

Tabla 1: Especificación de estereotipos de seguridad

Hemos propuesto una extensión de UML 2.0 mediante la cual es posible especificar requisitos de seguridad. En la Figura 2 se muestra, en color gris, los estereotipos relacionados con las especificaciones de seguridad en los diagramas de actividad. Mayores detalles acerca del estereotipo «*ActivitySecurityRequirement*» y sus clases derivadas puede encontrarse en [28]. En este trabajo profundizaremos sobre los estereotipos que están en color gris obscuro. Estos se relacionan directamente con el control de acceso y la identificación de roles y permisos.

El estereotipo *«ActivitySecurityElement»* (ver Tabla 1) es una clase abstracta creada para contener la especificación de algunos de los requisitos de seguridad considerados en la taxonomía propuesta en [14]. El estereotipo *«SecurityRole»* es una clase abstracta derivada de la clase Actor (from UseCase) que ha sido creada para contener las especificaciones de roles (ver Tabla 2). Este estereotipo tiene una relación de composición con el estereotipo *«AccessControl»*. El estereotipo *«SecurityPermission»* es una clase abstracta derivada de la clase Element (from Kernel) creada para contener la especificación de los permisos (ver Tabla 2). Los permisos deben ser especificados para cada uno de los objetos involucrados en el ámbito de una especificación de control de acceso.

Nombre	**SecurityRole**
Clase Base	Actor (from UseCases)
Descripción	Clase abstracta que contiene las especificaciones de roles
Restricciones	– *«SecurityRole»* sólo puede estar asociado al estereotipo *«AccessControl»*. – *«SecurityRole»* debe tener asociado un nombre – El Rol en *«SecurityRole»* puede ser obtenido desde las Actividades (Activity), Particiones (ActivityPartition) o Regiones (InterruptibleActivityRegion)
Nombre	**SecurityPermission**
Clase Base	Element (from Kernel)
Descripción	Clase abstracta que contiene las especificaciones de permisos
Restricciones	– *«SecurityPermission»* sólo puede estar asociado al estereotipo *«SecurityRole»* – *«SecurityPermission»* debe especificarse como un par *Objeto-Operación* – Un *Objeto* puede tener relación con una Acción (Action), un almacén de datos (DataStore) y/o un flujo de objetos (ObjectFlow). – Cada *Objeto* debe estar asociado a una *Operación,* de acuerdo con: – *Actions* {*Execution, CheckExecution*} *Execution* es el valor por defecto. *CheckExecution* es especificado cuando el Rol debe ser verificado una vez más antes de ejecutar la acción. – *DataStore {Update, Create, Read, Delete}* *Update* es el valor por defecto. Los valores *Create*, *Read* y *Delete* corresponden a la clásica definición de permisos sobre almacenes de datos. – *ObjectFlow {SendReceive , CheckSendReceive}* *SendReceive* es el valor por defecto. *CheckSendReceive* es especificado cuando el Rol debe ser verificado una vez más para poder llevar a cabo el envío/recepción del flujo

Tabla 2: Especificación de estereotipos de seguridad

4 Ejemplo

En nuestro ejemplo ilustrativo (ver Figura 3) hemos descrito un típico proceso de negocio para la admisión de pacientes en una institución de salud. En este caso, el analista de negocios ha identificado las siguientes Particiones: Paciente que corresponde a la persona que recibe la atención médica y que debe llenar una solicitud de admisión; Área de Administración (dividida en Admisión y Contabilidad) donde la institución médica registra los detalles acerca de los costos y seguros involucrados en la atención, y finalmente, Área Médica (dividida en Evaluación Médica y Exámenes) donde se llevan a cabo las pruebas de pre-admisión, evaluación y clínica y llenado de la ficha clínica de cada Paciente.

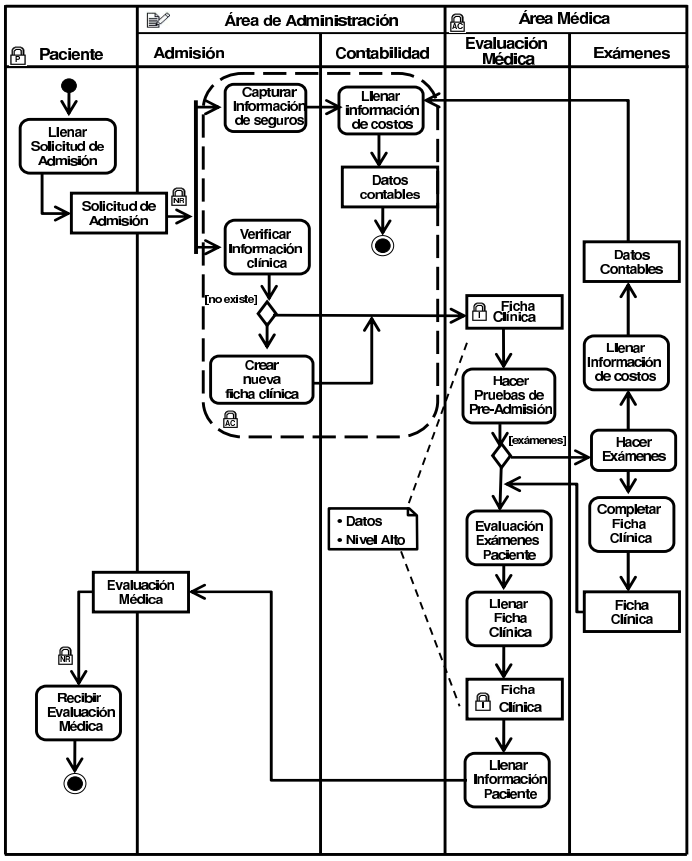


Fig. 3: Proceso de Negocio para la admisión de pacientes en una institución de salud

	Permisos		
Roles	**Objetos**		**Operaciones**
Admisión/Contabilidad	Action	Capturar información de seguros Llenar información de costos Verificar información clínica Crear nueva Ficha Clínica	Execution CheckExecution Execution Execution
	Data Store:	Datos Contables	Update
Evaluación Médica	Action	Hacer prueba de Pre-Admisión Evaluación de exámenes del paciente Llenar Ficha Clínica Llenar información paciente	Execution Execution Execution Execution
	Data Store	Ficha Clínica	Update
Exámenes	Action	Llenar información de costos Hacer Exámenes Completar Ficha Clínica	CheckExcecution Execution CheckExecution
	Data Store	Datos Contables Ficha Clínica	Read, Create Read, Create

Tabla 3: Especificación de Roles y Permisos

De todas las especificaciones de seguridad indicadas por el analista de negocios, hemos puesto especial atención en el control de acceso. *«AccessControl»* ha sido definido para la región que involucra las particiones "Admisión" y "Contabilidad". Esta especificación involucra a las acciones: "Capturar información de seguros", "Verificar información clínica", "Crear nueva ficha clínica" y "Llenar información de costos" y el almacén de datos "Datos contables". También se ha especificado control de acceso sobre la partición "Área Médica", lo que implica que se debe aplicar este requisito de seguridad sobre todos lo objetos (Actions, DataStore y/o ObjectFlow) que estén contenidos en las particiones "Evaluación Médica" y "Exámenes".

En la Tabla 3 mostramos los detalles que se pueden extraer desde la especificación de control de acceso. La primera columna muestra los roles que han sido obtenidos desde la especificación de actividades, particiones o regiones. La segunda columna muestra los objetos que se encuentran en el ámbito de la especificación de control de acceso. Y en la última columna se presenta la información acerca de las operaciones que se pueden realizar sobre los objetos.

5 Conclusiones y trabajo futuro

La mejora en los lenguajes para el modelado de proceso de negocio, en especial sobre los diagramas de actividad de UML 2.0, hace posible considerar requisitos de seguridad a partir de etapas tempranas en el desarrollo de sistemas.

En este trabajo hemos presentado una extensión de UML 2.0 con la que es posible especificar requisitos de seguridad en los diagramas de actividad. Con ello ampliamos las opciones de expresar requisitos por parte de los analistas de negocio. Hemos puesto especial énfasis en el requisito control de acceso; ya que, a partir de esa especificación, es posible identificar los roles y permisos orientados a implementar RBAC.

Los pasos siguientes de esta investigación deben orientarse a la aplicación del enfoque MDA, de manera que sea posible pasar a modelos más concretos (por ejemplo, modelos de ejecución) que incluyan los requisitos de seguridad. Para ello, el trabajo futuro debe estar encaminado a enriquecer la especificación de la extensión de UML 2.0 complementándola con Reglas de Buena Formación y OCL. También es necesario incorporar el punto de vista del experto en seguridad para mejorar la especificación y hacer posible su implantación.

Agradecimientos

Esta investigación es parte de los proyectos DIMENSIONS (PBC-05-012-1), parcialmente financiado por el FEDER y por la Consejería de Educación y Ciencia de la Junta de Comunidades de Castilla-La Mancha, COMPETISOFT (concedido por CYTED) y RETISTIC (TIC2002-12487-E) otorgado por la "Dirección General de Investigación del Ministerio de Ciencia y Tecnología" (España).

Referencias

1. Artelsmair, C. y Wagner, R.; *Towards a Security Engineering Process*, The 7th World Multiconference on Systemics, Cybernetics and Informatics. Vol. VI. Orlando, Florida, USA. (2003). pp.22-27.
2. Atluri, V.; *Security for Workflow Systems*, Information Security Technical Report. Vol. 6 (2). (2001). pp.59-68.
3. Backes, M., Pfitzmann, B. y Waider, M.; *Security in Business Process Engineering*, International Conference on Business Process Management. Vol. 2678, LNCS. Eindhoven, The Netherlands. (2003). pp.168-183.
4. Bertino, E.; *RBAC models – concepts and trends*, Computers and Security. Vol. 22 (6). (2003). pp.511-514.
5. Bertino, E., Ferrari, E. y Atluri, V.; *A Flexible model Supporting the Specification and Enforcement of Role-Based Authorizations in Workflow Management Systems*, Second ACM Workshop on Role-Based Access Control, Fairfax (Virginia). (1997). pp.1-12.
6. Bock, C.; *UML 2 Activity and Action Models*, Journal of Object Technology. Vol. 2 (4), July-August. (2003). pp.43-53.
7. Bock, C.; *UML 2 Activity and Action Models, Part 2: Actions*, Journal of Object Technology. Vol. 2 (5), September-October. (2003). pp.41-56.
8. Botha, R. A. y Eloff, J. H. P.; *A framework for access control in workflow systems*, Information Management & Computer Security. Vol. 9/3. (2001). pp.126-133.
9. Caetano, A., Rito Silva, A. y Tribolet, J.; *Business Process Modeling with Objects and Roles*, 6th International Conference on Enterprise Information Systems (ICEIS 2004). Porto, Portugal. (2004). pp.109-114.
10. Caetano, A., Zacarias, M., Rito Silva, A. y Tribolet, J.; *A Role-Based Framework for Business Process Modeling*, 38th Hawaii International Conference on System Sciences (HICSS-38 2005). Big Island, HI, USA. (2005). pp.130-136.
11. Eriksson, H.-E. y Penker, M., *Business Modeling with UML*, OMG Press. (2001).
12. Ferraiolo, D. F., Sandhu, R., Gavrila, S. I., Kuhn, D. R. y Chandramouli, R.; *Proposed NIST standard for role-based access control*, ACM Transactions on Information and System Security (TISSEC). Vol. 4 (3). (2001). pp.224-274.
13. Firesmith, D.; *Engineering Security Requirements*, Journal of Object Technology. Vol. 2 (1), January-February. (2003). pp.53-68.
14. Firesmith, D.; *Specifying Reusable Security Requirements*, Journal of Object Technology. Vol. 3 (1), January-February. (2004). pp.61-75.
15. Giaglis, G. M.; *A Taxonomy of Business Process Modelling and Information Systems Modelling Techniques*, International Journal of Flexible Manufacturing Systems. Vol. 13 (2). (2001). pp.209-228.
16. Herrmann, G. y Pernul, G.; *Viewing Business Process Security from Different Perspectives*, 11th International Bled Electronic Commerce Conference. Slovenia. (1998). pp.89-103.
17. 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.
18. List, B. y Korherr, B.; *A UML 2 Profile for Business Process Modelling*, 1st International Workshop on Best Practices of UML (BP-UML 2005) at ER-2005. Klagenfurt, Austria. (2005).
19. Liu, P. y Chen, Z.; *An Extended RBAC Model for Web Services in Business Process*, IEEE International Conference on E-Commerce Technology for Dynamic E-Business (CEC-East'04). (2004). pp.100-107.
20. Lodderstedt, T., Basin, D. y Doser, J.; *SecureUML: A UML-Based Modeling Language for Model-Driven Security*, UML 2002 - The Unified Modeling Language, 5th International Conference. Vol. 2460. Dresden, Germany. (2002). pp.426-441.

21. 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.
22. Maña, A., Ray, D., Sánchez, F. y Yagüe, M. I.; *Integrando la Ingeniería de Seguridad en un Proceso de Ingeniería Software*, VIII Reunión Española de Criptología y Seguridad de la Información, RECSI'04. Leganés, Madrid. España. (2004). pp.383-392.
23. Mega; *Business process Modeling and Standardization*. In http://www.bpmg.org/downloads/Articles/Article-MEGA-BusinessProcessModeling&StandardizationEN.pdf. (2004).
24. Mouratidis, H., Giorgini, P. y Manson, G. A.; *When security meets software engineering: a case of modelling secure information systems*, Information Systems. Vol. 30 (8). (2005). pp.609-629.
25. Object Management Group; *Unified Modeling Language: Superstructure*, version 2.0, formal/05-07-04. In http://www.omg.org/docs/formal/05-07-04.pdf. (2005).
26. Podeswa, H., *B.O.O.M.: Business Object-Oriented Modeling for Business Analysts*, Thomson Course Technology Incorporated, (2005). 401 p.
27. Quirchmayr, G.; *Survivability and Business Continuity Management*, ACSW Frontiers 2004 Workshops. Dunedin, New Zealand. (2004). pp.3-6.
28. Rodríguez, A., Fernández-Medina, E. y Piattini, M.; *Integrating Security Requirement with a UML 2.0 Profile*, International Symposium on Frontiers in Availability, Reliability and Security in conjunction with ARES. Vienna, Austria. (2006). pp.670-677.
29. 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.
30. Roser, S. y Bauer, B.; *A Categorization of Collaborative Business Process Modeling Techniques*, 7th IEEE International Conference on E-Commerce Technology Workshops (CEC 2005). Munchen, Germany. (2005). pp.43-54.
31. Sandhu, R. y Samarati, P.; *Authentication, Access Control, and Audit*, ACM Computing Surveys. Vol. 28 Nº1 March 1996. (1996). pp.241-243.
32. Sandhu, R. S.; *Future Directions in Role-Based Access Control Models*, International Workshop on Information Assurance in Computer Networks: Methods, Models, and Architectures for Network Security. Vol. 2052. St. Petersburg, Russia. (2001). pp.22-26.
33. 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).
34. Störrle, H.; *Semantics and Verification of Data Flow in UML 2.0 Activities*, Electronic Notes in Theoretical Computer Science. Vol. 127 (4). (2005). pp.35-52.
35. Tryfonas, T. y Kiountouzis, E. A.; *Perceptions of Security Contributing to the Implementation of Secure IS*, Security and Privacy in the Age of Uncertainty, IFIP TC11 18th International Conference on Information Security (SEC2003). Vol. 250. Athens, Greece. (2003). pp.313-324.
36. W.M.P. van der Aalst, Hofstede, A. H. M. t. y Weske, M.; *Business Process Management: A Survey*, International Conference on Business Process Management (BPM 2003). Volume 2678 (LNCS). Eindhoven, The Netherlands. (2003). pp.1-12.
37. WfMC, *Workflow Management Coalition: Terminology & Glossary.*, (1999). p.65.
38. Zuccato, A.; *Holistic security requirement engineering for electronic commerce*, Computers & Security. Vol. 23 (1). (2004). pp.63-76.