JISBD 2008

13th Conference on Software Engineering and Databases

XIII Jornadas de Ingeniería del Software y Bases de Datos

Gijón (Spain), October 7-10 2008

EDITORS: Ana Moreira
María José Suárez-Cabal
Claudio de la Riva
Javier Tuya

13th Conference on Software Engineering and Databases

XIII Jornadas de Ingeniería del Software y Bases de Datos

Gijón (Spain), October 7-10 2008

EDITORS: Ana Moreira
María José Suárez-Cabal
Claudio de la Riva
Javier Tuya

Edita:
Ana Moreira
María José Suárez-Cabal
Claudio de la Riva
Javier Tuya

Filmación e impresión:
Gráficas Rigel

Depósito Legal:
AS - 5.236 - 08

ISBN:
978-84-612-5820-8

Volume Editors Details

Ana Moreira
Departamento de Informática
Faculdade de Ciências e tecnologia
Universidade Nova de Lisboa
2829-516 Caparica, Portugal
E-mail: amm@di.fct.unl.pt
URL: http://ctp.di.fct.unl.pt/~amm/

María José Suárez-Cabal
Departamento de Informática
Universidad de Oviedo
33204 Gijón, Spain
E-mail: cabal@uniovi.es

Claudio de la Riva
Departamento de Informática
Universidad de Oviedo
33204 Gijón, Spain
E-mail: claudio@uniovi.es
URL: http://www.di.uniovi.es/~claudio/

Javier Tuya
Departamento de Informática
Universidad de Oviedo
33204 Gijón, Spain
E-mail: tuya@uniovi.es
URL: http://www.di.uniovi.es/~tuya/

Preface

Celebrating 13 Years of JISBD

With the 2008 edition in Gijón (October 7 to 10), the Conference on Software Engineering and Databases (JISBD) celebrates 13 years of existence. Born as a forum where the Spanish community would publish their work, meet to discuss potential research collaborations and evaluate the progress of research projects funded by the Spanish Ministery of Science and Technology, JISBD has long since moved beyond its initial boundaries and crossed several oceans.

Presently, the conference has become an important reference for younger researchers, as well as a forum which the more experienced do not wish to miss. In recent years, JISBD has broadened its radius, accepting papers also in English and Portuguese, in addition to Spanish. This change, not only brought more conference participants, but also significantly increased the number of submissions and, principally, the quality of the submissions accepted.

The JISBD community is now self-sustained and continues to expand. The quality of work accepted is equivalent to that of other relevant international events. In recent years, it has been possible to edit a special volume of IEEE LA with extended versions of the best conference papers and this also is happening with the current edition. This special issue, together with the conference proceedings with ISBN, is a showcase of the quality of the work of JISBD.

One of the highlights of this conference has been the excellence of its keynote speakers. Many of the most admired international researchers and professionals have already been invited to address the JISBD participants.

Within this rich framework for scientific and technological interchange, the conference includes several satellite events. In addition to the presentation of high quality original papers in the main conference, the program includes tutorials, tool demonstrations and workshops for the discussion of innovative ideas and work in progress, as well as a forum to bring to a wider audience research work already published in prestigious journals or conference proceedings (with an acceptance rate below 25% and an impact factor above 0.5).

It is no exaggeration to claim that JISBD has been consolidating its position as a reference event where researchers and professionals of Software Engineering and Databases can get together to discuss results and share ideas. JISBD has become an important forum for collaboration between different strands and research groups, while continuing to offer its participants a well organized event with exceptional hospitality.

About this Edition

The increased global reach of JISBD is evident in the origin of papers received. This year, in addition to the two Iberian and ten Latin-American countries, submissions arrived also from China, France, Germany, India, Iran and Pakistan.

Of a total of 115 abstracts, 112 papers were submitted for review. Most papers were reviewed by three PC members, and several were reviewed by four. The program Committee accepted 30 full papers and selected 12 for presentation as short papers. The acceptance rate for full papers was approximately 25%.

The increasing success of the conference implies greater responsibilities in terms of guaranteeing independent judgement and ensuring compliance with international standards of ethics. For this reason, a greater effort has been made in recent years to avoid double submissions, a task made

more difficult by the fact that the conference accepts submissions in three languages. This year, three good papers were rejected due to double submission, in different languages to different events.

In addition to the accepted papers, the conference includes five workshops, one tutorial, nine tool demos, an industrial panel and also a forum to discuss important relevant work already published elsewhere.

A highlight of the conference is, without doubt, the excellence of the invited keynote speakers. This year is no exception and we are honoured indeed to receive Bashar Nuseibeh and Bran Selic.

Bashar Nuseibeh is an academic and researcher at the Open University in the UK and invited professor in various other universities, including Japan's National Institute of Informatics. Bashar chairs several international committees and is recognized also for industry work, including organizations such as the UK's National Air Traffic Services (NATS), Texas Instruments, Praxis Critical Systems, Philips Research Labs, and NASA.

Bran Selic was, for many years, a distinguished engineer and researcher at IBM, and currently heads a global consultancy based in Canada. He is internationally known for his work in large-scale industrial systems, and for his pioneering work in Model-Driven Development and Real-Time Embedded Systems.

Bahsar's keynote is entitled "*The five W's (and one "H") of Security: ... Software Engineering of Secure Systems"* while Bran's is on "*Model-Based Software Engineering: Expected and Unexpected Challenges*".

Acknowledgements

A very special word of thanks is due to Bashar and Bran for having accepted my invitation and for sharing all the participants their knowledge, experience and refined wit. I sincerely hope JISBD was also for them a gratifying and unique experience.

Acknowledgements are due to a multitude of collaborators without whom the conference could not have been a success. Firstly, the paper authors for the trust placed in the quality of JISBD as a conference that merited their submissions. Secondly, to the PC members, whose diligent review work ensured that the authors' trust continues to be justified.

For managing the submission and review process, I was fortunate to have the constant help of Juan Hernández and José Javier Berrocal; they were my guardian angels, constantly alert to deadlines and ready to help as necessary. A special thanks for the contribution of my "Executive Program Committee", Antonio Vallecillo, Juan Hernández, Miguel Toro, Vicente Pelechano and Xavier Franch.

Acknowledgement is due to the main conference organizers, especially to Javier Tuya and his co-chair, Claudio de la Riva, for their efficient handling of the numerous tasks that a conference of this size and quality entails. Thanks also to those responsible for the satellite events (in alphabetical order), António Rito Silva, Antonio Vallecillo, Gustavo Rossi, João Araújo, João Falcão e Cunha, José Berrocal, José Corrales, José García-Fanjul, João Miguel Fernandes, Lidia Fuentes and María José Suárez-Cabal.

Finally, a special word of thanks to the sponsors of this conference, without whose contribution the event would have been somewhat less charming (not to mention gastronomically less satisfying).

Ana Moreira
Program Committee Chair

Prefácio

Celebrando 13 Anos de JISBD

Com a edição de 2008 em Gijón (7-10 Outubro), a Conferência em Engenharia de Software e Bases de Dados (JISBD) celebra 13 anos de existência. Apesar de ter nascido como um fórum onde a comunidade espanhola publicava os seus trabalhos e se reunia para discutir potenciais colaborações futuras de investigação, e até avaliar o estado de andamento dos projectos de investigação financiados pelo Ministério da Ciência e Tecnologia espanhola, há muito que extravasou essas fronteiras e cruzou oceanos.

Actualmente o JISBD é um marco importante na investigação dos mais jovens, mas também um fórum que os mais seniores não querem perder. Nos últimos anos a conferência abriu-se para o mundo inteiro, aceitando artigos escritos em Inglês, Espanhol e Português. Esta viragem trouxe não só mais participantes à conferência, mas também um aumento significativo do número de trabalhos submetidos e, principalmente, um aumento na qualidade desses trabalhos.

A comunidade do JISBD é agora auto-sustentada e em contínua expansão. A qualidade dos trabalhos aceites é equiparada à de muitos outros eventos internacionais de relevo. Por este motivo, nos últimos anos, foi-nos possível editar um volume especial no IEEE LA com uma versão estendida dos melhores trabalhos da conferência, o que acontecerá também nesta edição. Este volume, em conjunto com as actas formais da conferência com ISBN, é uma montra da qualidade do trabalho que aqui se discute.

Uma das características de excelência desta conferência tem sido, desde sempre, o gabarito dos seus palestrantes convidados. É um prazer ver que muitos dos mais admirados investigadores e profissionais internacionais já foram convidados a falar para os participantes do JISBD.

Neste enquadramento fecundo para divulgação científica e tecnológica, a conferência inclui vários eventos satélite. Além dos artigos seleccionados para apresentação na conferência, o programa inclui ainda tutoriais, demonstrações de ferramentas, workshops para discussão de ideias inovadores e trabalhos em andamento, assim como um evento para a disseminação de trabalho de investigação já publicado em revistas e actas de conferências de grande prestígio (onde o índice de aceitação é inferior a 25% e o factor de impacto superior a 0.5).

Assim, não é excessivo afirmar que o JISBD se tem vindo a consolidar como um evento de referência onde investigadores e profissionais em Engenharia de Software e Bases de Dados se encontram para discutir, disseminar e trocar ideias, partilhar experiências e resultados entre diversos sectores e grupos de investigação, num contexto de excelente organização e invulgar hospitalidade.

Sobre esta Edição

A atestar o crescimento e internacionalização do JISBD está a origem dos artigos que nos chegaram. Este ano, a nacionalidade dos autores foi surpreendentemente diversificada, pois para além dois países Ibéricos e de dez países Latino-Americanos, recebemos trabalhos também da Alemanha, China, França, Índia, Irão e Paquistão.

O número total de resumos foi de 115, sendo que destes, 112 artigos foram submetidos para avaliação. Cada artigo foi avaliado por pelo menos três revisores, sendo que vários foram avaliados por quatro. O Comité de Programa aceitou 30 artigos longos e escolheu 12 para apresentação como artigos curtos. Assim, o índice de aceitação de artigos longos foi de cerca de 25%.

Este sucesso acarreta responsabilidades acrescidas em garantir a independência de julgamentos e em fazer cumprir a ética e as normas internacionais. É por este motivo que, nos últimos anos, se

tem feito um esforço muito grande para evitar submissões duplicadas, tarefa nem sempre fácil para os membros do Comité de Programa, já que a conferência aceita três línguas de escrita. Este ano foram rejeitados três bons artigos avaliados como de submissão duplicada, em duas línguas, para eventos diferentes.

Para além dos artigos seleccionados, a conferência conta também com a organização de cinco *workshops*, um *tutorial*, nove demonstrações de ferramentas, um painel industrial e ainda um fórum onde se discutem trabalhos de relevo já publicados em revistas ou outras conferências.

Mas sem dúvida que os momentos mais altos da conferência são sempre marcados pelo admirável conjunto de palestrantes convidados. Este ano tivemos a sorte de receber Bashar Nuseibeh e de Bran Selic.

Bashar Nuseibeh é um académico e investigador da Open University, na Inglaterra, e professor convidado em várias outras universidades, incluindo o Instituto Japonês de Informática. Bashar preside vários comités internacionais e é admirado também pelo seu trabalho para a indústria, que inclui organizações como o National Air Traffic Services (NATS) do Reino Unido, Texas Instruments, Praxis Critical Systems, Philips Research Labs, e a NASA.

Bran Selic foi durante umas dezenas de anos engenheiro e investigador distinguido da IBM e actualmente preside uma empresa de consultoria internacional sediada no Canadá. É conhecido mundialmente pelos seus trabalhos em sistemas de larga escala industrial e também pelo seu pioneirismo nas áreas de desenvolvimento orientado a modelos e sistemas embutidos de tempo real.

A palestra do Bashar é intitulada "*The five W's (and one "H") of Security: ... Software Engineering of Secure Systems"*, enquanto que a do Bran é sobre "*Model-Based Software Engineering: Expected and Unexpected Challenges*".

Agradecimentos

Uma palavra especial de agradecimento ao Bashar e ao Bran por terem aceite o meu convite e por brindarem todos os participantes com a sua experiência, conhecimento e refinado sentido de humor. Espero que o JISBD tenha sido também para eles uma experiência agradável e diferente.

Agradecimentos são justamente devidos ao grande número de colaboradores, sem o contributo dos quais, a conferência não poderia ter tido êxito. Aos autores, claro, por confiarem na qualidade do JISBD e submeterem, por isso, os seus trabalhos. Aos membros do Comité de Programa cujas revisões asseguram que essa confiança continua a justificar-se.

Para gerir o sistema de submissão, contei com o apoio incondicional do Juan Hernández e do José Javier Berrocal. Eles foram os meus "anjos da guarda", sempre atentos a todos os prazos e prontos a dar todas as explicações. Um agradecimento particular ao contributo meu "Comité Executivo de Programa", Antonio Vallecillo, Juan Hernández, Miguel Toro, Vicente Pelechano e Xavier Franch. Obrigada pelo vosso apoio e sugestões.

Obrigada aos organizadores principais da conferência, em especial ao Javier Tuya, e ao seu vice-presidente, Claudio de la Riva, pela gestão eficaz das inúmeras tarefas que uma conferência desta dimensão exige. Um agradecimento é ainda devido, e por ordem alfabética, aos responsáveis dos eventos satélite, António Rito Silva, Antonio Vallecillo, Gustavo Rossi, João Araújo, João Falcão e Cunha, José Berrocal, José Corrales, José García-Fanjul, João Miguel Fernandes, Lidia Fuentes e María José Suárez-Cabal.

Finalmente, um agradecimento aos patrocinadores da conferência, sem o contributo de quem o evento teria tido menos charme (e uma gastronomia muito menos requintada).

Ana Moreira
Presidente do Comité de Programa

Prefacio

Con esta edición 2008 en Gijón (7 al 10 de Octubre), las Jornadas de Ingeniería del Software y Bases de Datos (JISBD) celebra 13 años de existencia. JISBD nació como un foro donde la comunidad española publicaba su trabajo, discutía potenciales colaboraciones en investigación y evaluaba el progreso de los proyectos de investigación financiados por el Ministerio de Ciencia y Tecnología, y en la actualidad ha traspasado fronteras y cruzado varios océanos.

Actualmente, la conferencia es una referencia importante para jóvenes investigadores, así como un foro de cita obligada para investigadores más experimentados. Durante los últimos años, JISBD se ha abierto al mundo, aceptando artículos en Inglés y Portugués, además de Castellano. Este cambio no solamente se ha traducido en más participantes, sino que ha incrementado significantemente el número de artículos enviados, y principalmente, la calidad de los artículos aceptados.

La comunidad JISBD está actualmente auto sustentada y continúa expandiéndose. La calidad de los trabajos aceptados es equivalente al de otros eventos internacionales relevantes. Durante los últimos años, ha sido posible editar un volumen especial de IEEE LA con versiones ampliadas de los mejores trabajos presentados en la conferencia, lo que sucederá también en la presente edición. Este volumen especial, junto con las actas de la conferencia con ISBN, es una muestra de la calidad de los trabajos de JISBD.

Una de las características más sobresalientes de la conferencia ha sido la calidad de los ponentes invitados. Varios investigadores y profesionales de reconocido prestigio internacional han sido invitados a participar como ponentes en JISBD.

Dentro de este marco científico y tecnológico, la conferencia incluye varios eventos relacionados. Además de la presentación de artículos originales de alta calidad en la conferencia principal, el programa incluye tutoriales, demostraciones de herramientas, talleres para la discusión de ideas innovadoras y trabajos en curso, así como la divulgación de trabajos de investigación publicados en revistas y conferencias de prestigio (con un ratio de aceptación por debajo del 25% y un factor de impacto por encima de 0,5).

No es una exageración afirmar que JISBD ha consolidado su posición como un evento de referencia donde investigadores y profesionales de la Ingeniería del Software y las Bases de Datos se reúnen para discutir resultados y compartir ideas. JISBD se ha convertido en un foro importante para la colaboración entre diferentes sectores y grupos de investigación, en un contexto de excelente organización y excepcional hospitalidad.

Sobre la presente edición

El crecimiento e internacionalización de JISBD se hace evidente analizando el origen de los artículos recibidos. En la presente edición, además de los artículos recibidos de los dos países de la Península Ibérica y los diez países Latinoamericanos, se han recibido artículos de China, Francia, Alemania, India, Irán y Pakistán.

De un total de 115 resúmenes previamente recibidos, finalmente se recibieron 112 artículos para su revisión. La mayoría de los artículos fueros revisados por tres miembros del Comité de Programa y varios por cuatro. El Comité de Programa aceptó 30 artículos largos y seleccionó 12 para su presentación como artículos cortos. El ratio de aceptación para los artículos largos fue de aproximadamente el 25%.

El éxito de la conferencia implica grandes responsabilidades en términos de garantizar la independencia de las revisiones y el cumplimiento de los estándares internacionales de ética. Por esta razón, durante los últimos años se ha realizado un mayor esfuerzo en aras de evitar envíos duplicados, una tarea especialmente dificultosa, ya que la conferencia acepta envíos en tres idiomas. En la

presente edición tres artículos fueron rechazados debido al doble envío en diferentes idiomas para diferentes eventos.

Además de los artículos aceptados, la conferencia incluye cinco talleres, un tutorial, nueve demostraciones de herramientas y foro para la discusión y divulgación de trabajos relevantes previamente publicados, así como una mesa redonda de carácter industrial.

Una característica importante de la conferencia es, sin ninguna duda, la excelencia de los ponentes invitados. La presente edición no es una excepción y estamos orgullosos de contar con la presencia de Bashar Nuseibeh y Bran Selic.

Bashar Nuseibeh es académico e investigador en la Open Unversity del Reino Unido y profesor invitado en otras muchas universidades, incluyendo el Instituto Nacional Japonés de Informática. Bashar preside varios comités internacionales y está reconocido igualmente por su trabajo industrial, incluyendo organizaciones tales como el Servicio Nacional de Tráfico Aéreo del Reino Unido (NATS), Texas Instruments, Praxis Critical Systems, Philips Research Labs y la NASA.

Bran Selic fué durante varios años un destacado ingeniero e investigador en IBM y actualmente lidera un consultora internacional con sede en Canadá. Es internacionalmente conocido por su trabajo en sistemas industriales a gran escala y por su trabajo pionero en Desarrollo Dirigido por Modelos y Sistemas Empotrados en Tiempo Real.

La conferencia de Bashar se titula "*The five W's (and one "H") of Security: ... Software Engineering of Secure Systems"* y la de Bran "*Model-Based Software Engineering: Expected and Unexpected Challenges*".

Agradecimientos

Un agradecimiento especial es para Bashar y Bran por haber aceptado mi invitación y por compartir con todos los participantes sus conocimientos, experiencia y refinado sentido del humor.

Agradecimientos también para la multitud de colaboradores sin los cuales el éxito de la conferencia no habría sido posible. En primer lugar, para los autores de los artículos por confiar en la calidad de JISBD y enviar sus trabajos. En segundo lugar, para los miembros del Comité de Programa, cuyas revisiones aseguran la calidad de los trabajos.

Para el proceso de gestión y revisión de los trabajos recibidos, fui afortunada por tener la ayuda constante de Juan Hernández y José Javier Berrocal. Ellos fueron mis ángeles guardianes, alertándome constantemente de las fechas límite y siempre preparados para ayudarme cuando lo necesitaba. Agradecimientos especiales por la contribución de mi "Comité de Programa Ejecutivo", Antonio Vallecillo, Juan Hernández, Miguel Toro, Vicente Pelechano y Xavier Franch.

Agradecimientos también para los organizadores de la conferencia principal, especialmente al presidente del comité organizador Javier Tuya y su vicepresidente Claudio de la Riva, por su manejo eficiente de las numerosas tareas que una conferencia de este tamaño y calidad conllevan. Agradecimientos también para los responsables de los eventos relacionados (en orden alfabético) António Rito Silva, Antonio Vallecillo, Gustavo Rossi, João Araújo, João Falcão e Cunha, José Berrocal, José Corrales, José García-Fanjul, João Miguel Fernandes, Lidia Fuentes y María José Suárez-Cabal.

Finalmente, palabras especiales de agradecimiento para los patrocinadores de la conferencia, sin cuya contribución el evento habría sido menos encantador (y con una gastronomía menos refinada).

Ana Moreira
Presidenta del Comité de Programa

Conference Committee

Program Committee Chair
Ana Moreira (Univ. Nova de Lisboa, Portugal)

Organizing Chair
Javier Tuya (Univ. Oviedo, Spain)

Organizing Co-Chair
Claudio de la Riva (Univ. Oviedo, Spain)

Permanent Committee Secretary
Mario Piattini (Univ. Castilla-La Mancha, Spain)

Tutorial Chair
António Rito Silva (Univ. Técnica Lisboa, Portugal)

Workshop Chair
João Araújo (Univ. Nova de Lisboa, Portugal)

Tool Demonstrations Chair
Lidia Fuentes (Univ. Málaga, Spain)

Relevant Papers Dissemination Chairs
Antonio Vallecillo (Univ. Málaga, Spain)
João Falcão Cunha (Univ. Porto, Portugal)

Proceedings Chair
María José Suárez-Cabal (Univ. Oviedo, Spain)

Cyber Chair
Jose Javier Berrocal (Univ. Extremadura, Spain)

Web Chair
José A. Corrales (Univ. Oviedo, Spain)

Publicity Chairs
Gustavo Rossi (Univ. La Plata, Argentina)
José García-Fanjul (Univ. Oviedo, Spain)
João Miguel Fernandes (Univ. Minho, Portugal)

Organizing Committee (Univ. Oviedo, Spain)

Javier Tuya
Claudio de la Riva
José García-Fanjul
Isabel Sevilla
María José Suárez-Cabal
José Ramón de Diego
Raquel Blanco
Eugenia Díaz Fernández
José A. Corrales
Marta Fernández de Arriba

SISTEDES Executive Board

President
Miguel Toro (Univ. Sevilla, Spain)

Vice President
Juan José Moreno (Univ. Polit. Madrid, Spain)

Secretary
Nieves R. Brisaboa (Univ. Coruña, Spain)

Treasurer
Javier Tuya (Univ. Oviedo, Spain)

Members
Pere Botella (Univ. Polit. Catalunya, Spain)
Ricardo Peña (Univ. Complutense Madrid, Spain)
Coral Calero (Univ. Castilla-La Mancha, Spain)
Manuel Hermenegildo (Univ. Polit. Madrid, Spain)
Ernesto Pimentel (Univ. Málaga, Spain)
María Ribera Sancho (Univ. Polit. Catalunya, Spain)
Natalia Juristo (Univ. Polit. Madrid, Spain)
Salvador Lucas (Univ. Polit. Valencia, Spain)

Submission and Review Support System
(Quercus Software Engineering Group)

Javier Berrocal (Univ. Extremadura, Spain)
Juan Hernández (Univ. Extremadura, Spain)

Secretariat

Fundación Universidad de Oviedo
C/ Principado 3, 4ª Planta
33007 Oviedo, Spain.
Tel: 34-985104927
Fax: 34-985104928

Executive Program Committee

Xavier Franch (Univ. Polit. Catalunya, Spain)
Juan Hernández (Univ. Extremadura, Spain)
Vicente Pelechano (Univ. Polit. Valencia, Spain)
Antonio Vallecillo (Univ. Málaga, Spain)
Miguel Toro (Univ. Sevilla, Spain)
Javier Tuya (Univ. Oviedo, Spain)

Program Committee

Albert Abelló (Univ. Polit. Catalunya, Spain)
Ana Paula Afonso (Univ. Lisboa, Portugal)
Ademar Aguiar (Univ. Porto, Portugal)
Jesús Aguilar (Univ. Sevilla, Spain)
José Aldana (Univ. Málaga, Spain)
Mauricio Alférez (U. Nova de Lisboa, Portugal)
Bárbara Álvarez (Univ. Polit. Cartagena, Spain)
Raquel Anaya (Univ. EAFIT, Colombia)
María José Aramburu (Univ. Jaume I, Spain)
Hernán Astudillo (U. T. Federico Santa María, Chile)
Orlando Belo (Univ. do Minho, Portugal)
Rafael Berlanga (Univ. Jaume I, Spain)
Paulo Borba (Univ. Federal Pernambuco, Brazil)
Pere Botella (Univ. Polit. Catalunya, Spain)
Rosana Braga (Univ. São Paulo, Brazil)
Nieves Brisaboa (Univ. Coruña, Spain)
Isabel Brito (Inst. Polit. Beja, Portugal)
Fernando Brito e Abreu (U. Nova de Lisboa, Portugal)
Coral Calero (Univ. Castilla-La Mancha, Spain)
Marcelo Campo (UNICEN, Argentina)
Carlos Canal (Univ. Málaga, Spain)
Valeria de Castro (Univ. Rey Juan Carlos, Spain)
Matilde Celma (Univ. Polit. Valencia, Spain)
Christina Chávez (Univ. Bahia, Brazil)
Rafael Corchuelo (Univ. Sevilla, Spain)
Dolors Costal (Univ. Polit. Catalunya, Spain)
Yania Crespo (Univ. Valladolid, Spain)
Carlos Delgado (Univ. Carlos III, Spain)
Oscar Díaz (Univ. País Vasco, Spain)
Javier Dolado (Univ. País Vasco, Spain)
Xavier Franch (Univ. Polit. Catalunya, Spain)
Pablo de la Fuente (Univ. Valladolid, Spain)
Mario Gaspar da Silva (Univ. Lisboa, Portugal)
Alessando García (Univ. Lancaster, UK)
Marcela Genero (Univ. Castilla-La Mancha, Spain)
Cristina Gómez (Univ. Polit. Catalunya, Spain)
Jaime Gómez (Univ. Alicante, Spain)
Alfredo Goñi (Univ. País Vasco, Spain)
Silvia Gordillo (UNLP, Argentina)
Pedro Guerreiro (Univ. Algarbe, Portugal)
Juan Hernández (Univ. Extremadura, Spain)
Jon Iturrioz (Univ. País Vasco, Spain)
Elena Jurado (Univ. Extremadura, Spain)
Natalia Juristo (Univ. Polit. Madrid, Spain)
Miguel Katrib (Grupo WEBOO, Cuba)
María Lencastre (Univ. Pernambuco, Brazil)
Antonia Lopes (Univ. Lisboa, Portugal)
Adolfo Lozano (Univ. Extremadura, Spain)
Esperanza Marcos (Univ. Rey Juan Carlos, Spain)
Henrique Madeira (Univ. Coimbra, Portugal)
Eduardo Mena (Univ. Zaragoza.Spain)
Ana María Moreno (Univ. Polit. Madrid, Spain)
Juan José Moreno (Univ. Polit. Madrid, Spain)
Juan Manual Murillo (Univ. Extremadura, Spain)
Oscar Pastor (Univ. Polit. Valencia, Spain)
Vicente Pelechano (Univ. Polit. Valencia, Spain)
Marcelo Pimenta(Univ. F. Rio Grande do Sul, Brazil)
Ernesto Pimentel (Univ. Málaga, Spain)
Mónica Pinto (Univ. Málaga, Spain)
Ángeles Places (Univ. Coruña, Spain)
Antonio Polo (Univ. Extremadura, Spain)
Claudia Pons (UNICEN, Argentina)
Tom Price (Univ. F. Rio Grande do Sul, Brazil)
Carme Quer (Univ. Polit. Catalunya, Spain)
Celia Ramos (Univ. Algarbe, Portugal)
Isabel Ramos (Univ. Sevilla, Spain)
Isidro Ramos (Univ. Polit. Valencia, Spain)
Claudio de la Riva (Univ. Oviedo, Spain)
José Riquelme (Univ. Sevilla, Spain)
José Luis Roda (Univ. La Laguna, Spain)
María José Rodríguez Fortis (Univ. Granada, Spain)
José Raúl Romero (Univ. Córdoba, Spain)
Antonio Ruiz (Univ. Sevilla, Spain)
Francisco Ruiz (Univ. Castilla-La Mancha, Spain)
José Samos (Univ. Granada, Spain)
Fernando Sánchez (Univ. Extremadura, Spain)
Juan Sánchez (Univ. Polit. Valencia, Spain)
Carla Silva (Univ. F. Pernambuco, Brazil)
Ernest Teniente (Univ. Polit. Catalunya, Spain)
Miguel Toro (Univ. Sevilla, Spain)
Ambrosio Toval (Univ. Murcia, Spain)
Juan Carlos Trujillo (Univ. Alicante, Spain)
Toni Urpi (Univ. Polit. Catalunya, Spain)
Antonio Vallecillo (Univ. Málaga, Spain)
Belén Vela (Univ. Rey Juan Carlos, Spain)

Referees

Álvaro E. Prieto Ramos
Amador Durán Toro
André L. Santos
Andrea Delgado
Ángel Herranz
Angélica Caro
Anna Grimán Padua
Antonio Jesús Roa Valverde
Antônio Oliveira Filho
Antonio Ruiz-Cortés
Arturo Zambrano
Carlos Bobed
Carlos D. Barranco González
Carlos Enrique Cuesta Quintero
Carlos Neil
Cecilia Delgado Negrete
César J. Acuña
Claudio Sant`Anna
Cristina Vicente Chicote
Daniel Rodríguez
Dante Carrizo
Diana Marcela Sánchez
Diego Alonso Cáceres
Diego Seco Naveiras
Domingo Savio Rodríguez Baena
Eduardo Rodríguez López
Elisa Yumi Nakagawa
Ellen Francine Barbosa
Encarna Sosa Sánchez
Fernando Molina Molina
Fran J. Ruiz Bertol
Francisco Javier Lucas Martínez
Francisco Luís Gutiérrez Vela
Francisco Martínez Álvarez
Ignacio García Rodríguez de Guzmán
Ismael Caballero
Ismael Navas Delgado
Ismael Sanz Blasco
Javier Pérez García
Joaquín Lasheras
Joaquín Nicolás
Jorge Gracia
Jorge Martínez Gil
José María Cavero Barca
Juan Ángel Pastor Franco
Juan M. Vara
Juan Manuel Pérez Martínez
Manuel Ángel Serrano Martín
Manuel Resinas
Márcio de Medeiros Ribeiro
Marcirio Chaves
Marcos López Sanz
Mari Carmen Otero
María Esperanza Manso Martínez
María Luisa Rodríguez Almendros
María Teresa Gómez López
María Visitación Hurtado Torres
Martin Solari
Miguel Ángel Laguna Serrano
Miguel Ángel Martínez
Miguel Rodríguez Luaces
Mª Ángeles Moraga de la Rubia
Nuno Cardoso
Orlando Avila-García
Oscar Dieste
Óscar Pedreira Fernández
Othmane Chniber
Pablo Inostroza
Pablo Trinidad
Paloma Cáceres García de Marina
Pedro Sánchez Palma
Raquel M. Crespo García
Raquel Trillo Lado
Roberto Almeida Bittencourt
Roberto Rodríguez Echeverría
Roberto Ruiz
Rui Lopes
Sascha Ossowski
Sergio Ilarri Artigas
Vicente Luque Centeno

Sponsors


Universidad de Oviedo
400
cuarto centenario


PCTI
ASTURIAS


Ayuntamiento de Gijón


GOBIERNO DE ESPAÑA
MINISTERIO DE CIENCIA E INNOVACIÓN


GOBIERNO DEL PRINCIPADO DE ASTURIAS


TIC
CLUSTER ASTURIAS


csc


InterSystems


cajAstur


DEPARTAMENTO DE INFORMATICA
UNIVERSIDAD DE OVIEDO


Sistedes
Sociedad de Ingeniería del Software y Tecnologías de Desarrollo de Software


gijon.info

Table of Contents[1]

[1] The section headings below correspond to the conference program, but do not include all the presentations in each conference session (where short papers and dissemination papers on the same topic also were included). Thus, the sections here all contain fewer papers than the corresponding conference session; the short papers are listed separated in this volume, followed by a chapter with an overview of the dissemination papers.

Information Engineering

Model Engineering

Formal Methods

Maintenance and Testing

Data Mining, Data Streaming and Datawarehouses

Reengineering and Software Modernization

Quality, Measurement & Estimation of Products & Processes

Requirements Engineering

Keynote Address 2

Short Papers

Workshops, Tutorials, Demos and Dissemination

Gestión de la Variabilidad de los Requisitos de Seguridad en Líneas de Producto Software

Daniel Mellado[1], Eduardo Fernández-Medina[2] y Mario Piattini[2]

[1] Ministerio de Trabajo e Inmigración, Gerencia de Informática de la Seguridad Social, Madrid (España)
Daniel.Mellado@alu.uclm.es
[2] Universidad de Castilla La-Mancha, Departamento de Tecnologías y Sistemas de Información, Grupo de investigación ALARCOS,
Paseo de la Universidad, 4 13071 Ciudad Real (España)
{Eduardo.FdezMedina,Mario.Piattini}@uclm.es

Resumen. Actualmente las líneas de producto son cada vez más comunes y se está extendiendo su aplicación en la industria del software y por lo tanto aumentando también el número de líneas que se desarrollan en las que la seguridad es un aspecto crítico. Sin embargo, las propuestas existentes en líneas de producto están enfocadas fundamentalmente a la gestión de los requisitos y variabilidad funcional en lugar de a la gestión de los requisitos de seguridad y su variabilidad, factor crítico de éxito en cualquier línea. Es por esto que en este artículo se presenta una propuesta de gestión sistemática de la variabilidad de los requisitos de seguridad desde las primeras fases del ciclo de vida de desarrollo de una línea de producto software con el objetivo de facilitar la conformidad de los productos de la línea con los estándares de seguridad más importantes relativos a la gestión de requisitos de seguridad, como la ISO/IEC 15408 (Criterios Comunes) y la ISO/IEC 27001.

Palabras Clave: Ingeniería de requisitos de seguridad, Líneas de producto, Variabilidad.

1 Introducción

Hoy en día para poder alcanzar los niveles deseados de calidad y mejorar la productividad, multitud de sistemas se están desarrollando basándose en el paradigma de ingeniería de Líneas de Producto Software (LPS), ya que las LPS ayudan a reducir significativamente el tiempo de puesta en producción y los costes de desarrollo, mediante la reutilización de todo tipo de artefactos [2, 4].

Debido a la complejidad y a la naturaleza extensiva propia de las LPS, la seguridad y la ingeniería de requisitos son mucho más importantes para la puesta en práctica del desarrollo basado en LPS, de lo que ya son para el desarrollo de un Sistema de Información (SI), ya que una brecha de seguridad o vulnerabilidad en la línea puede provocar importantes problemas a largo plazo a todos los productos de la misma [14]. Es por ello que la disciplina conocida como Ingeniería de Requisitos de Seguridad [16], sea una parte muy importante en el proceso de desarrollo software y especialmente dada su complejidad para conseguir LPS seguras, ya que facilitan técnicas, métodos y normas para abordar esta tarea desde las primeras fases del desarrollo e implica el uso de procedimientos repetibles y sistemáticos para asegurar que el conjunto de requisitos obtenidos es completo, consistente y fácilmente comprensible y analizable por parte de los diferentes actores implicados en el desarrollo de la LPS y sus sistemas. Asimismo, las metodologías de ingeniería del software y los estándares propuestos para ingeniería de LPS tradicionalmente han tratado someramente los temas relativos a los requisitos de seguridad y la variabilidad de la seguridad.

Después de analizar en [20, 21] las propuestas más recientes y relevantes relativas a los requisitos de seguridad en SI como: [6, 8, 19, 26, 28, 29], junto con las propuestas más importantes sobre gestión de requisitos en LPS, como [4, 14, 15, 25, 27], así como las arquitecturas de seguridad de referencia para LPS, como [1, 5, 9], llegamos a la conclusión de que las propuestas existentes estaban más orientadas a la solución en lugar de a la ingeniería de requisitos de seguridad. De forma que dichas propuestas no proporcionaban una gestión de requisitos de seguridad en LPS sistemática e intuitiva que facilitara la trazabilidad y variabilidad de estos requisitos, ni especificaban su gestión en los modelos de ingeniería de LPS. Por ello, hemos desarrollado el proceso de ingeniería de requisitos de seguridad para LPS, llamado SREPPLine (Security Requirements Engineering Process for software Product Lines) [23], cuyo objetivo es facilitar una integración concreta de las actividades relativas a la gestión de requisitos de seguridad en el resto de actividades del desarrollo basado en LPS y proporcionar un soporte metodológico específico para la gestión de requisitos de seguridad y del modelo de variabilidad de seguridad de la línea. Asimismo, ayuda a que las LPS y los sistemas que de ella se deriven sean conformes respecto a la gestión de requisitos de seguridad con los estándares de seguridad internacionales más importantes (como ISO/IEC 15408, ISO/IEC 17799 o ISO/IEC 27001), aspecto último del que identificamos que tampoco ayudaban las propuestas existentes en este ámbito de la ingeniería de LPS.

En este artículo, con el objetivo de tratar de resolver los aspectos mejorables en las propuestas actuales de gestión de la variabilidad en los requisitos de seguridad en LPS, se presentan el Modelo de Decisión de Requisitos de Seguridad y el Modelo de Variabilidad de la Seguridad como una extensión al proceso SREPPLine presentado en [23], donde se describió el proceso y sus flujos, pero sin detallar la gestión de la variabilidad de la seguridad ni estos modelos mediante los que se gestiona y que son soportados por el Repositorio de Recursos de Seguridad que plantea SREPPLine. Dichos modelos, complementarios entre sí, constituyen el modelo de gestión de la variabilidad de los requisitos de seguridad de SREPPLine y tienen el propósito de ayudar en la reutilización de los requisitos de seguridad y sus artefactos relacionados así como dar soporte a la gestión de las características, requisitos de seguridad y demás artefactos relacionados variables y comunes, es decir, la finalidad de estos modelos es gestionar la trazabilidad y variabilidad de los requisitos de seguridad y la de sus artefactos relacionados desde las primeras fases del ciclo de vida de desarrollo de una LPS de manera sistemática. A través del Modelo de Decisión de Requisitos de Seguridad que está dirigido por estándares de seguridad (ISO/IEC 15408 e ISO/IEC 27001) se ayuda en la conformidad y/o certificación frente a estos estándares de seguridad a los productos o sistemas que se deriven de la LPS.

El resto del artículo está organizado de la siguiente forma: en la sección 2, se describe de forma general el proceso SREPPLine. Seguidamente en la sección 3, se describirá la gestión de la variabilidad de los requisitos de seguridad en SREPPLine presentándose el Modelo de Decisión de Requisitos de Seguridad y el Modelo de Variabilidad de la Seguridad. Y por último, en la sección 4, presentamos nuestras conclusiones y trabajos futuros.

2 Descripción General de SREPPLine: Proceso de Ingeniería de Requisitos de Seguridad para Líneas de Producto Software

El Proceso de Ingeniería de Requisitos de Seguridad para Líneas de Producto Software (SREPPLine) [23] es un add-in de actividades (que se descomponen en tareas, donde se generan artefactos de entrada y salida, y con la participación de distintos roles) que se integran sobre el proceso de desarrollo de LPS existente en una organización, proporcionándole un enfoque en ingeniería de requisitos de seguridad específico para LPS. Los sub-procesos y actividades descritos en este artículo se pueden combinar con los procesos de desarrollo como el Proceso Unificado u otros. En este artículo se considera la gestión de la variabilidad de los requisitos de seguridad en

SREPPLine en combinación con el marco de trabajo de ingeniería de LPS propuesto por Pohl et al. en [25].

SREPPLine se trata de un proceso de ingeniería de requisitos de seguridad especializado para el desarrollo de LPS, basado en las características ('features') y metas de seguridad y dirigido por el riesgo y los estándares de seguridad ISO/IEC 15408 e ISO/IEC 27001, que gestiona los requisitos de seguridad y sus artefactos relacionados desde las primeras fases del desarrollo de una LPS o de un producto miembro de ésta de forma sistemática. Para ello se apoya en la utilización de las últimas técnicas de requisitos de seguridad (como los casos de mal uso [28] o los casos de uso de seguridad [7]), así como en la integración de los componentes de los Criterios Comunes (CC) o ISO/IEC 15408 [11] y de los controles de la ISO/IEC 27001 [12] en el ciclo de desarrollo de la LPS con el fin de facilitar la certificación de seguridad de los productos miembros de la LPS. Asimismo, este proceso propone la utilización de un método de análisis y gestión de riesgos que sea conforme a la norma ISO/IEC 13335 [10], de hecho el proceso esta particularizado para la utilización de Magerit [18] tanto para la estimación de riesgos de la LPS como de sus productos miembros.

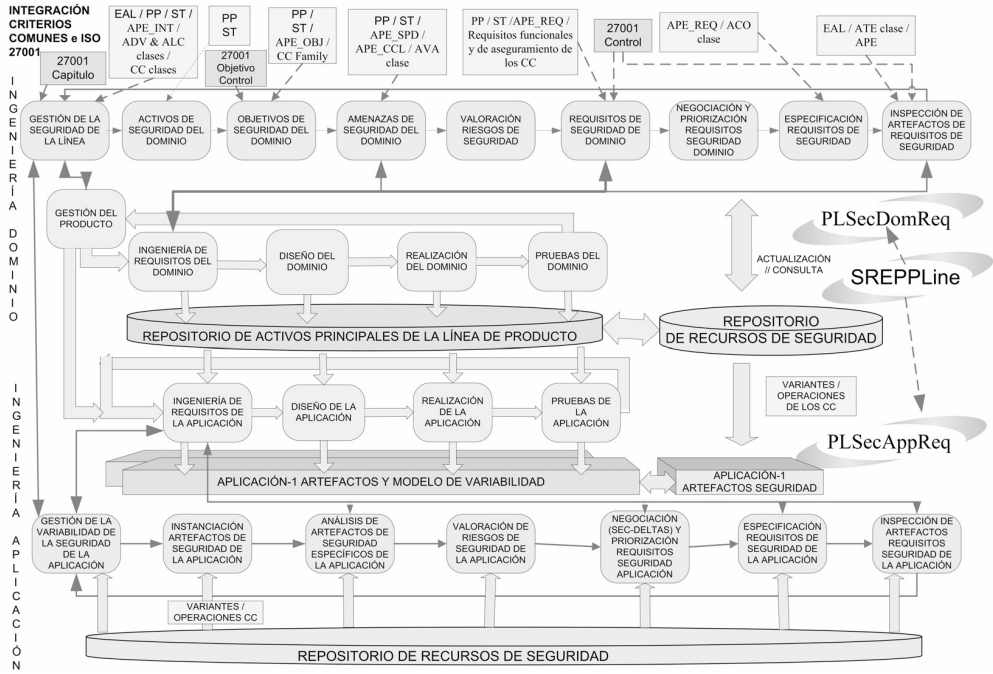

Fig. 1 Marco de Trabajo para la Ingeniería de Requisitos de Seguridad en Líneas de Producto

SREPPLine busca minimizar la participación de los expertos de seguridad en el desarrollo de los productos de la LPS y el conocimiento necesario de los estándares de seguridad. Para conseguirlo, como se observa en la Fig. 1, utiliza un Repositorio de Recursos de Seguridad integrado con el repositorio de activos principales de la LPS para facilitar la reutilización de los artefactos de seguridad de la LPS y para implementar el Modelo de Variabilidad de la Seguridad y el Modelo de Decisión de Requisitos de Seguridad, los cuales ayudan a gestionar la variabilidad y la trazabilidad de los artefactos de seguridad entre sí, así como entre los de las aplicaciones con los de la línea, a la vez que dan soporte a la elicitación y razonamiento integral de requisitos de seguridad en la ingeniería de LPS. El modelo de variabilidad de seguridad implementado por SREPPLine se apoya en el concepto de modelo de variabilidad ortogonal [25], lo cual nos permite flexibilidad para aplicarlo, ya que facilita que el proceso se integre con otros modelos de desarrollo software (como modelos de 'features', de casos de uso, de diseño, o modelos de componentes o de pruebas).

Como se puede observar en la Fig. 1, SREPPLine se compone de dos sub-procesos con sus respectivas actividades: PLSecDomReq (Product Line Security Domain Requirements Engineering sub-process) y PLSecAppReq (Product Line Security Application Requirements Engineering sub-process). Estos sub-procesos cubren las cuatro fases básicas de la ingeniería de requisitos [16]: elicitación de requisitos; análisis y negociación de requisitos; documentación de requisitos; y validación y verificación de requisitos. Dichos sub-procesos se ejecutarán al menos por cada iteración del proceso de ingeniería del dominio y/o de la aplicación de la LPS, respectivamente.

3 Gestión de la Variabilidad de los Requisitos de Seguridad en SREPPLine

Las propuestas existentes de gestión de la variabilidad en LPS están enfocadas fundamentalmente a la gestión de la variabilidad de la funcionalidad y no suelen considerar la gestión de los requisitos de seguridad como otro de los aspectos fundamentales, especialmente en aquellos sistemas donde la seguridad es un factor esencial. Es por ello que en SREPPLine se propone un Repositorio de Recursos de Seguridad que sirva de soporte al Modelo de Decisión de Requisitos de Seguridad y al Modelo de Variabilidad de la Seguridad. Estos modelos, complementarios entre sí, constituyen el modelo de gestión de la variabilidad de los requisitos de seguridad de SREPPLine y tienen el propósito de ayudar en la reutilización de los requisitos de seguridad y sus artefactos relacionados, así como dar soporte a la gestión de las características, requisitos de seguridad y demás artefactos relacionados variables y comunes, es decir, gestionar la variabilidad de los requisitos de seguridad en el ciclo de vida de la LPS junto con sus preceptivos enlaces de trazabilidad o trazas asociadas. En esencia, se trata de un repositorio de conocimiento con una estructura que facilite la elicitación y razonamiento integral de requisitos de seguridad en LPS.

El Modelo de Variabilidad de la Seguridad está integrado en el Modelo de Decisión de Requisitos de Seguridad y se utiliza para ayudar en la gestión de la variabilidad y trazabilidad de los requisitos de seguridad y artefactos relacionados de la LPS y sus productos o sistemas, así como facilitar la conformidad y/o certificación frente a los estándares de seguridad ISO 15408 e ISO 27001. El Modelo de Decisión de Requisitos de Seguridad da soporte a la captura, especificación y razonamiento de los requisitos de seguridad y sus artefactos relacionados, al igual que también es útil en el proceso de selección de los estándares de seguridad y establecimiento de los requisitos de seguridad más apropiados para la LPS o sistema de ésta. Además, posibilita la creación de un Perfil de Protección (conforme a la ISO 15408 o Criterios Comunes) en función de las metas de seguridad de la LPS o producto/sistema miembro de ésta.

A continuación se explican ambos modelos que gestionan la variabilidad en SREPPLine únicamente de manera teórica por motivos de espacio, en [22] se describe un caso de estudio de aplicación de SREPPLine que realizamos en una Administración Pública española y en el que se ejemplifica la aplicabilidad de estos modelos.

3.1 Modelo de Variabilidad de la Seguridad

Este Modelo de Variabilidad de la Seguridad que planteamos y que se muestra en la Fig. 1 está basado en la Especificación de Activos Reutilizables (RAS, Reusable Assets Specification) adoptado como estándar OMG [24], a la vez que extiende el modelo de variabilidad ortogonal propuesto por Pohl et al [25]. Asimismo, este modelo se integra dentro del Modelo de Decisión de Requisitos de Seguridad como parte del mismo, pero por motivos de una mejor comprensión se explican de manera separada.

Este modelo de variabilidad que proponemos, debido a que extiende el modelo de variabilidad ortogonal de Pohl, permite definir la variabilidad de la seguridad de la LPS y relacionarla a través de las trazas con los otros modelos de desarrollo software y de LPS, como los modelos de

características, modelos de casos de uso, modelos de diseño, modelos de componentes y modelos de pruebas. De esta forma nos ayuda a documentar la variabilidad de la seguridad de una manera común a lo largo de los diferentes modelos sin tener que modificar las notaciones existentes, con lo que es más sencillo de integrarlo en la metodología de desarrollo de LPS de un Departamento de Informática de una Organización. Además, nos proporciona una visión transversal de la variabilidad de la seguridad en todos los niveles del desarrollo, y por lo tanto de todos los artefactos de seguridad de la LPS y sus productos, así como ayuda a que las diferentes vistas de la variabilidad de los artefactos de los requisitos de seguridad sean consistentes entre sí y con el resto de artefactos de desarrollo, ya que con esta trazabilidad se ofrece un soporte controlado para la modificación y extensión de la línea o de sus aplicaciones miembro.

Los elementos básicos que conforman el Modelo de Variabilidad de la Seguridad se definen usando UML 2 en el meta-modelo subyacente a éste y que se muestra en la Fig. 2. Los tres elementos principales del modelo de variabilidad ortogonal [25] son las clases: "punto de variación", "variante" y "artefacto".

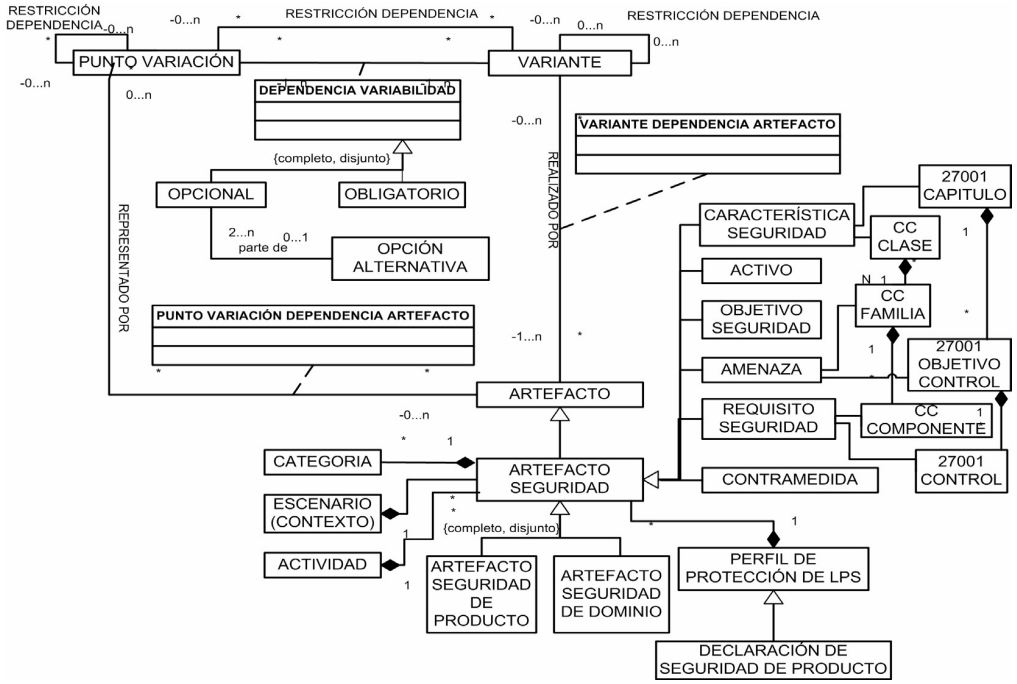

Fig. 2 Meta-modelo de Variabilidad de la Seguridad

La clase asociación "dependencia de variabilidad" relaciona un punto de variación con al menos una variante y viceversa, es decir, una variante con al menos un punto de variación. Ésta puede ser una relación obligatoria u opcional. La relación de dependencia de variabilidad obligatoria establece que una variante es obligatoria para el punto de variación al que está relacionado. Esto no implica que esta variante tenga que incluirse en todos los productos / aplicaciones de las LPS, ya que una variante obligatoria es parte de un producto / aplicación solo si su punto de variación al que está asociado es parte del producto, por lo tanto dicho punto de variación puede que no sea parte de una de las características obligatorias de todas las aplicaciones de la línea. La relación de dependencia de variabilidad opcional establece que una variante relacionada a un punto de variación que puede ser parte de alguna aplicación de la LPS pero puede no ser necesariamente parte de dicha aplicación. La relación de elección alternativa agrupa un conjunto de variantes que están relacionadas a través de una dependencia de variabilidad opcional al mismo punto de variación y define el rango del número de variantes opcionales que pueden seleccionarse para ese grupo.

La asociación "restricción de dependencia variante a punto de variación" describe una relación entre una variante y un punto de variación donde la selección de una variante requiere o excluye la consideración de un punto de variación. La asociación "restricción de dependencia de variante" describe una relación entre dos variantes de tal manera que la selección de una variante requiere o excluye la selección de otra variante independientemente de los puntos de variación a los que las variantes estén asociadas. Análogamente, la asociación "restricción de dependencia de punto de variación" describe una relación entre dos puntos de variación, donde un punto de variación requiere o excluye la consideración de otro punto de variación para ser totalmente completo.

También es importante relacionar a través de las trazas la variabilidad de la seguridad de la LPS definida en el Modelo de Variabilidad de la Seguridad con los otros modelos de desarrollo software. Es por ello que el meta-modelo que se muestra en la Fig. 2 contiene la clase "artefacto", la cual representa a cualquier tipo de artefacto de desarrollo. Artefactos específicos de desarrollo son sub-clases de la clase "artefacto", como por ejemplo la clase "artefacto de seguridad" que es una especialización de la clase artefacto. Un "artefacto" puede pero no tiene por qué estar relacionado a una o más variantes, pero una variante si que tiene que estar relacionada con al menos un artefacto de desarrollo. Asimismo, un artefacto puede pero no tiene por qué estar relacionado con uno o varios puntos de variación, al igual que un punto de variación puede pero no tiene por qué estar relacionado con uno o más artefactos.

Por lo tanto, el Repositorio de Recursos de Seguridad que se representa en la Fig. 1, debe de estar integrado en el repositorio de activos principales de la LPS con el fin de facilitar las trazas entre el modelo de variabilidad de la LPS y los diferentes tipos de artefactos de seguridad y demás artefactos de desarrollo.

Como se puede observar en la Fig. 2, la clase "artefacto de seguridad" tiene una relación de especialización completa y disjunta de manera que todo artefacto de seguridad tiene que ser un artefacto de seguridad de una aplicación de la LPS o bien un artefacto de seguridad propio del dominio de la LPS. Cada "artefacto de seguridad" forma parte del conjunto de artefactos de desarrollo asociados a una actividad del proceso de desarrollo, sin embargo una actividad puede pero no tiene por qué estar relacionada con uno o varios artefactos de seguridad. Asimismo, un "artefacto de seguridad" debe de ser parte de un "escenario", es decir, debe tener un contexto, aunque el escenario pude pero no tiene por qué estar relacionado con uno o varios artefactos de seguridad. Además, un artefacto de seguridad pude pero no tiene por qué estar categorizado. La clase "categoría" nos ayuda a prevenir problemas semánticos y facilita la reutilización de artefactos de seguridad e incluso la utilización de patrones de seguridad. Se trata de una clase fundamental para el Modelo de Decisión de Requisitos de Seguridad, porque estas categorías de los artefactos de seguridad sirven de guía en la identificación de los artefactos de seguridad de las aplicaciones / productos así como de nuevas LPS. Esta reusabilidad del producto nos garantizará ciclos de desarrollo más rápidos basados en soluciones probadas. La clase "artefacto de seguridad" tiene como obligatorio el atributo "versión" con el objetivo de facilitar la trazabilidad y variabilidad de las versiones de los artefactos de seguridad, e incluso permitir que haya aplicaciones / productos con diferentes versiones del mismo artefacto de seguridad.

Por último, en la Fig. 2 se representa la variabilidad de los estándares de seguridad, describiéndose la integración de los elementos de los Criterios Comunes y los controles de la ISO/IEC 27001 en el Modelo de Variabilidad de la Seguridad. Estos elementos de los estándares de seguridad están asociados con las categorías de algunos artefactos de seguridad concretos (características / 'features' de seguridad, amenazas y requisitos de seguridad) con el fin de ayudar a la certificación sistemática de la LPS o de sus productos en estos estándares (ISO/IEC 15408 o ISO/IEC 27001) y hacer más sencilla su argumentación y razonamiento, utilizándose en conjunción con el Modelo de Decisión de Requisitos de Seguridad, como se explicará en el siguiente apartado.

3.2 Modelo de Decisión de Requisitos de Seguridad

Los artefactos de seguridad los tratamos como una fuente natural de variabilidad entre las aplicaciones / productos o los artefactos de la LPS. Por lo tanto, con el objetivo de capturar y gestionar el conocimiento relacionado con los requisitos de seguridad proponemos la definición de un Modelo de Decisión de Requisitos de Seguridad que de soporte a la ingeniería de LPS. El meta-modelo que subyace de este Modelo de Decisión de Requisitos de Seguridad está representado en la Fig. 3, por motivos de una mejor comprensibilidad no incluye el Modelo de Variabilidad de la Seguridad que es complementario a éste.

Este modelo facilita la elicitación y razonamiento de los artefactos de los requisitos de seguridad así como la conformidad con los estándares de seguridad ISO/IEC 27001 e ISO/IEC 15408. Da soporte a la captura, especificación, razonamiento y argumentación de los requisitos de seguridad tanto de la LPS como de los miembros de la línea.

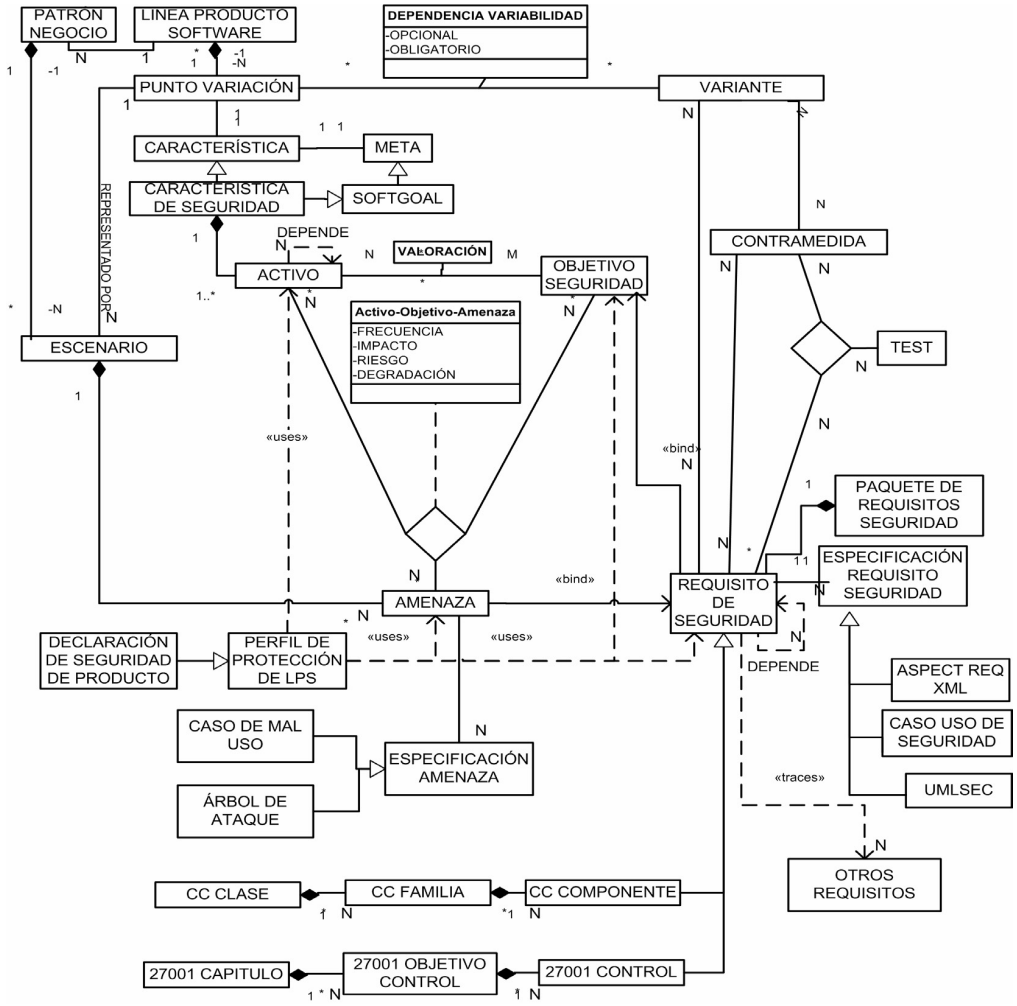

Fig. 3 Meta-modelo de Decisión de Requisitos de Seguridad

La reusabilidad del proceso soportada por este modelo nos permitirá aplicarlo a diferentes dominios, dentro del contexto de los desarrollos basados en LPS, mientras que la reusabilidad del producto que aporta el Repositorio de Recursos de Seguridad nos garantizará ciclos de desarrollo más rápidos basados en soluciones probadas. Además, este Modelo de Decisión de Requisitos de

Seguridad facilita la interoperabilidad del producto, consistente en la identificación, a partir de las metas y características de seguridad, de los requisitos de seguridad en términos de restricciones de seguridad lógicas, físicas y organizativas, y más tarde en contramedidas y controles concretos, durante el diseño de la LPS, y de la asignación, para cada uno de los requisitos de seguridad identificados, de los controles de seguridad propuestos por uno o más estándares de gestión de requisitos de seguridad como ISO/IEC 15408 o ISO/IEC 27001.

En términos de ingeniería de requisitos de seguridad, este modelo tiene como objetivo principal la construcción de Sistemas de Información (de productos de la LPS) en los que esté cuidadosamente balanceado el riesgo con el impacto de implementación de los requisitos de seguridad en los miembros de la LPS, es decir, con el coste económico de la implementación de las contramedidas asociadas a los requisitos de seguridad. Sin embargo, ni este modelo propuesto ni el proceso SREPPLine pretenden ser una herramienta de análisis y gestión de riesgos, aunque si que para realizar esta tarea el modelo contempla la utilización de una metodología de análisis de riesgos ya existente conforme con la ISO/IEC 13335, en concreto se plantea Magerit [18] como metodología de análisis de riesgos.

Como punto de partida utilizamos las metas o las metas débiles ("softgoals") [3] y los modelos de características y sus correlaciones para tener en cuenta tanto a los requisitos funcionales como a los no funcionales, concretamente a los requisitos de seguridad. Para expresar las intenciones del sistema pueden utilizarse tanto los modelos de metas como los modelos de características, y en la mayoría de los casos definen información similar [25]. Por lo tanto, el interés de utilizar un modelo complementario de metas al de características es debido al hecho de que nos permite añadir intencionalidad, es decir, decidir (siempre que las trazas estén definidas correctamente) qué características de seguridad son necesarias para satisfacer las metas de seguridad seleccionadas y cuál es el conjunto óptimo de características de seguridad de una determinada prioridad en el contexto de los distintos escenarios de la LPS, proporcionando así razonamiento al proceso de selección. Esto supone en la práctica un mayor nivel de abstracción del proceso de selección de las variantes de seguridad de la LPS, haciendo que la selección de las características de seguridad de la LPS o de la aplicación / producto se haga a nivel de requisitos en lugar de a nivel de diseño.

Además, en este modelo se caracteriza a la LPS como un conjunto de "puntos de variación" que son representados por "características" (features) o metas y cada meta pude alcanzarse por varios caminos concretos, representados por "escenarios".

Los conceptos principales en los que se basa este modelo son: característica de seguridad (security feature), activo, objetivo de seguridad, amenaza, requisito de seguridad y perfil de protección de la LPS. Otros conceptos de seguridad complementarios que maneja son: riesgo, impacto, degradación, frecuencia, contramedida y conceptos de estándares de seguridad (de los Criterios Comunes o ISO/IEC 15408 y de la ISO/IEC 27001).

Las características de seguridad son aquellas características ('features') que describen atributos de seguridad del sistema que se corresponden con las metas de seguridad que el sistema (aplicación o LPS) en construcción debería alcanzar. De esta manera, en general habrá un grupo de activos involucrado en la satisfacción de cada meta de seguridad y sus características de seguridad asociadas.

Estos activos son los elementos del sistema de información de la LPS o estrechamente relacionados con éste que aportan valor a la organización y que son necesarios para su funcionamiento correcto y la consecución de los objetivos propuestos por su dirección. Asimismo, distinguimos varias categorías o tipos de activos (como entorno, sistema de información, servicios, componentes e información o datos).Un activo, como se observa en la Fig. 3, es una clase que hereda de la clase "artefacto de seguridad" con lo que pude ser un punto de variación y puede tener dependencias con otros activos. Cada activo tiene relacionados diferentes objetivos de seguridad (o dimensiones de seguridad) con su correspondiente valoración (siguiendo una escala normalizada de 0 a 10 según la metodología Magerit [18] que es la que SREPPLine propone para realizar el análisis de riesgos) acordada por las partes interesadas ('stakeholders'), los cuales tienen también que llegar a un acuerdo sobre los activos comunes y opcionales. Se da una valoración para cada objetivo de seguridad de cada activo y se propaga a través de las trazas de dependencia por el árbol

de activos, de forma que basta con que se valore explícitamente los activos jerárquicamente más altos en el árbol de dependencias.

Los objetivos o dimensiones de seguridad son los objetivos que deben alcanzarse para proteger las metas de negocio de la organización. Siguiendo Magerit [18], los objetivos o dimensiones de seguridad que el modelo gestiona pueden ser únicamente los siguientes: integridad de los datos, confidencialidad de los datos, disponibilidad, autenticidad de los usuarios del servicio, autenticidad del origen de los datos, trazabilidad del servicio, y trazabilidad de los datos. Este Modelo de Decisión de Requisitos de Seguridad facilita la identificación y valoración de los objetivos de seguridad para cada activo del sistema (producto o LPS), mediante la selección de la categoría/s de cada activo, proporcionando los objetivos de seguridad relacionados con estas categorías que contiene el Repositorio de Recursos de Seguridad de la organización.

Además, los activos están expuestos a amenazas que pueden impedir que se satisfagan los objetivos de seguridad asociados a estos activos. Pero no todas las amenazas afectan a todos los activos ni a todos los objetivos de seguridad para todas las aplicaciones de la LPS, con lo que se tienen que identificar las amenazas comunes y opcionales. Asimismo, existe cierta relación entre el tipo o categoría del activo y lo que le puede suceder a éste. De esta manera, mediante la adecuada identificación y selección de la categoría/s del activo este modelo de decisión propuesto puede sugerir amenazas o categorías de amenazas relacionadas con la categoría/s del activo seleccionadas, dando así soporte a la identificación de las amenazas comunes y variables y a su valoración. Para calcular el impacto de cada amenaza el modelo tiene en cuenta el valor de cada activo para cada objetivo de seguridad y el factor de degradación que causaría la materialización de la amenaza sobre el activo. Para realizar la valoración del riesgo, se considera tanto el impacto de la amenaza como su frecuencia de ocurrencia. Después, el modelo registra el riesgo clasificándolo en un rango normalizado según Magerit [18] de 0 (casi nulo) a 5 (muy alto).

Cada categoría o tipo de activo, dependiendo de sus categorías de amenazas asociadas, tiene asociada alguna/s categorías de requisitos de seguridad que puedan mitigar el impacto de sus amenazas asociadas o bien reducir su frecuencia de ocurrencia. Este mecanismo que implementa el Modelo de Decisión de Requisitos de Seguridad, facilita la identificación de los requisitos de seguridad comunes y variables de la LPS así como la selección de los requisitos de seguridad variables o bien la identificación de los específicos y particulares de cada aplicación de la LPS. También permite mantener la consistencia de las distintas relaciones de trazabilidad y variabilidad entre la LPS y sus miembros.

Adicionalmente, pueden existir dependencias entre requisitos de seguridad con lo que el modelo contempla el concepto de "paquete de requisitos de seguridad" que están estructurados por objetivo de seguridad que tratan de garantizar. Es decir, son un grupo de requisitos de seguridad que trabajan de forma conjunta para mitigar el mismo tipo de amenazas y satisfacer objetivos de seguridad comunes sobre unos activos dados. Sin embargo, puede haber ciertos grupos de requisitos de seguridad dentro del grupo que difieran entre sí por el nivel de detalle que describen y por el nivel de comprobación de su satisfacción que soportan. Por lo tanto, es necesario, y el modelo así lo contempla, que se puedan definir jerarquías de requisitos de seguridad a través de las trazas de dependencia.

Las metas de seguridad pueden alcanzarse mediante múltiples requisitos de seguridad (es decir, por distintas variantes). La correspondencia entre los requisitos de seguridad con sus contramedidas se realiza de tal manera que se consiga el mejor efecto posible sobre los activos asociados a las características y metas de seguridad. De esta forma, una variante se materializa en uno o más requisitos de seguridad, los cuales son implementados por una o más contramedidas. Las contramedidas son los procedimientos y mecanismos técnicos que se identifican en la fase de diseño y cuyo fin es reducir el riesgo, se tratan en definitiva de decisiones arquitectónicas que se usan para alcanzar las metas de seguridad.

Como también se explicó en el Modelo de Variabilidad de la Seguridad (Fig. 2), este Modelo de Decisión de Requisitos de Seguridad como se muestra en la Fig. 3, integra elementos de los estándares de seguridad ISO/IEC 15408 (Criterios Comunes) e ISO/IEC 27001 con el fin de facilitar la conformidad y la certificación de la LPS y de sus miembros contra estos estándares a la

vez que simplificar su argumentación y razonamiento, ayudando en la identificación y documentación adecuada de los requisitos de seguridad y demás artefactos de seguridad relacionados. Para conseguirlo, como se puede observar en la Fig. 2 en este modelo a través del Modelo de Variabilidad de la Seguridad se relacionan las categorías de ciertos artefactos de seguridad (características de seguridad, amenazas y requisitos de seguridad) con elementos concretos de los Criterios Comunes (ISO/IEC 15408) y de la ISO/IEC 27001.El Modelo de Decisión de los Requisitos de Seguridad (Fig. 3) contempla el concepto de Perfil de Protección de la LPS, como un conjunto de requisitos de seguridad y sus artefactos de seguridad relacionados, independiente de la implementación para una categoría o dominio de sistemas de información que satisfacen unas metas de seguridad determinadas. Por tanto, el modelo permite asociar Perfiles de Protección de LPS con Patrones de Negocio. Todo ello para facilitar la certificación de la LPS contra los Criterios Comunes. Análogamente, el Modelo de Decisión de Requisitos de Seguridad utiliza el concepto de Declaración de Seguridad del Producto, entendido como un conjunto de requisitos de seguridad y sus artefactos de seguridad relacionados, implementados de forma particularizada para un miembro / producto de la LPS y que satisfacen las metas de seguridad de dicho producto / aplicación.

Como se puede ver en la Fig. 3, en el Modelo de Decisión de Requisitos de Seguridad se utilizan los escenarios para representar las variantes, asimismo dichos escenarios tienen un entorno o contexto que debería incluir aspectos tales como: activos, actores, atacantes o usuarios mal intencionados, casos de uso, casos de mal uso [28] o amenazas, y casos de uso de seguridad [6]. Los modelos de características contienen variabilidad ya por sí mismos. Sin embargo, definir la variabilidad de un árbol de características mediante el modelo de variabilidad ortogonal [25], como permite este modelo, mejora las capacidades de expresividad del árbol y nos ayuda a documentar la variabilidad de la seguridad de una manera común a lo largo de los diferentes modelos sin tener que modificar las notaciones existentes. Para el modelado de las amenazas el modelo permite el uso de plantillas de casos de mal uso o de árboles de ataque para documentar y registrar la variabilidad de dichos artefactos. Los requisitos de seguridad pueden documentarse mediante plantillas de casos de uso de seguridad, estereotipos adicionales de UMLsec [13], o como requisitos textuales usando una especificación XML orientada a aspectos [17].

El modelo de variabilidad ortogonal en el que nuestro modelo se basa nos permite relacionar entre si las distintas partes en las que se define la variabilidad. Gracias a esto, partiendo de un artefacto de seguridad modificado siguiendo sus trazas se puede encontrar inmediatamente los otros artefactos de seguridad y de desarrollo que pueden estar afectados por el cambio, a través de la relación con su variante asociada y de la relación de la variante con sus otros artefactos asociados. De esta manera, la variabilidad de los artefactos de seguridad del Modelo de Decisión de Requisitos de Seguridad queda documentada de forma clara y no ambigua gracias a las trazas de dependencias de los artefactos de seguridad del modelo de gestión de la variabilidad de los requisitos de seguridad que se propone. Además, mediante estas trazas del modelo que planteamos, se pueden tener registradas las decisiones tomadas en lo relativo a la seguridad junto con los artefactos implicados que justifican dichas decisiones.

4 Conclusiones

Los requisitos de seguridad son extremadamente importantes en las LPS debido a que una brecha de seguridad en la línea puede provocar graves problemas a los productos de ésta a lo largo de su ciclo de vida. A pesar de que recientemente se han desarrollado diversas propuestas que tratan de salvar las distancias entre la ingeniería de requisitos y la ingeniería de requisitos en LPS, no existe una propuesta disponible que sistematice la definición de requisitos de seguridad de calidad y gestione la variabilidad de estos requisitos y de sus artefactos relacionados en los modelos de LPS.

Por tanto, la contribución principal de este trabajo es la de proporcionar, como una extensión de SREPPLine [23], una propuesta de gestión sistemática de la variabilidad de los requisitos de

seguridad desde las primeras fases del ciclo de vida de desarrollo de una LPS con el fin de facilitar la conformidad de los productos de la LPS con los estándares de seguridad más importantes relativos a la gestión de requisitos de seguridad, como la ISO/IEC 15408 (Criterios Comunes) y la ISO/IEC 27001. Nuestra propuesta define un Modelo de Decisión de Requisitos de Seguridad dirigido por estándares de seguridad que ayuda en la definición de los requisitos de seguridad y facilita la certificación y conformidad de los productos de las LPS frente a los anteriormente mencionados estándares de seguridad. Dicho modelo junto con el Modelo de Variabilidad de la Seguridad facilitan la gestión de la variabilidad y trazabilidad sistemática de los requisitos de seguridad y sus artefactos relacionados a lo largo del ciclo de vida de la LPS o de un producto miembro de ésta. Estos modelos que planteamos nos proporcionan una visión transversal de la variabilidad de la seguridad en todos los niveles del desarrollo, y por lo tanto de todos los artefactos de seguridad de la LPS y sus productos, así como ayuda a que las diferentes vistas de la variabilidad de los artefactos de los requisitos de seguridad sean consistentes entre sí y con el resto de artefactos de desarrollo. Con lo que posibilita que la selección de las características de seguridad de la LPS o de la aplicación se haga a nivel de requisitos en lugar de a nivel de diseño. Es por ello que SREPPLine junto con la extensión propuesta en este artículo está especialmente indicado para aquellas LPS en las que la seguridad es un aspecto de calidad crítico, dado el gran impacto que puede suponer en este tipo de líneas la existencia o no de determinadas metas o características de seguridad en todos los miembros de la línea, así como el nivel de gestión de la variabilidad de las características de seguridad requerida para los diversos segmentos de mercado.

Por último, como consecuencia una de las lecciones aprendidas destacadas en el caso de estudio de aplicación de SREPPLine que realizamos en una Administración Pública descrito en [22], estamos trabajando en refinar un prototipo de herramienta CARE (Computer Aided Requirements Engineering) que hemos desarrollado para dar soporte a SREPPLine y que implementa los modelos expuestos en este artículo, para asistir y automatizar la compleja gestión y mantenimiento de las relaciones de variabilidad y trazabilidad de los artefactos que se generan en SREPPLine y mejorar así la eficiencia del proceso de ingeniería de requisitos de seguridad de LPS. Asimismo, tenemos planeado el refinamiento tanto del modelo teórico como del prototipo de la herramienta a partir de la realización de más casos de estudio que estamos realizando, con el objetivo final de proporcionar un marco de trabajo integral de ingeniería de requisitos de seguridad en LPS.

Agradecimientos

Este artículo es parte de los proyectos ESFINGE (TIN2006-15175-C05-05) y ELEPES (TIN2006-27690-E) del Ministerio de Educación y Ciencia, y de los proyectos QUASIMODO (PAC08-0157-0668), MISTICO (PBC-06-0082) y MELISA (PAC08-0142-335) del FEDER y de la Consejería de Ciencia y Tecnología de la Junta de Comunidades de Castilla- La Mancha.

Referencias

1. Arciniegas, J.L., Dueñas, J.C., Ruiz, J.L., Cerón, R., Bermejo, J., and Oltra, M.A., *Architecture Reasoning for Supporting Product Line Evolution: An Example on Security*, in *Software Product Lines: Research Issues in Engineering and Management*, Käkölä, T. and Dueñas, J.C., Editors. 2006, Springer.
2. Bosh, J., *Design & Use of Software Architectures*. 2000: Pearson Education Limited.
3. Chung, L., Nixon, B., Yu, E., and Mylopoulos, J., *Non-Functional Requirements in Software Engineering*. 2000: Kluwer Academic Publishers.
4. Clements, P. and Northrop, L., *Software Product Lines: Practices and Patterns*. SEI Series in Software Engineering. 2002: Addison-Wesley.
5. Faegri, T.E. and Hallsteinsen, S., *A Software Product Line Reference Architecture for Security*, in *Software Product Lines: Research Issues in Engineering and Management*, Käkölä, T. and Dueñas, J.C., Editors. 2006, Springer.

6. Firesmith, D.G., *Security Use Cases*. Journal of Object Technology, 2003: p. 53-64.
7. Firesmith, D.G., *Specifying Reusable Security Requirements*. Journal of Object Technology, 2004: p. 61-75.
8. Giorgini, P., Massacci, F., Mylopoulos, J., and Zannone, N. *ST-Tool: A CASE Tool for Security Requirements Engineering*. in *IEEE International Conference on Requirements Engineering (RE'05)*. 2005.
9. Immonen, A., *A Method for Predicting Reliability and Availability at the Architecture Level*, in *Software Product Lines: Research Issues in Engineering and Management*, Käkölä, T. and Dueñas, J.C., Editors. 2006, Springer.
10. ISO/IEC, *ISO/IEC 13335 Information technology - Security techniques - Management of information and communications technology security - Part 1: Concepts and models for information and communications technology security management*. 2004.
11. ISO/IEC, *ISO/IEC 15408:2005 Information technology - Security techniques - Evaluation criteria for IT security, (Common Criteria v3.0)*. 2005.
12. ISO/IEC, *ISO/IEC 27001 Information technology -- Security techniques -- Information security management systems -- Requirements*. 2006.
13. Jürjens, J., *UMLsec: extending UML for secure systems development*. UML 2002 - The Unified Modeling Language. Model Engineering, Languages,Concepts, and Tools. 5th International Conference., 2002. **LNCS 2460**: p. 412-425.
14. Käkölä, T. and Dueñas, J.C., *Software Product Lines: Research Issues in Engineering and Management*. 2006: Springer.
15. Kim, J., Kim, M., and Park, S., *Goal and scenario bases domain requirements analysis environment*. The Journal of Systems and Software, **79**(7) (2005). p. 926 - 938.
16. Kotonya, G. and Sommerville, I., *Requirements Engineering Process and Techniques*. Hardcover ed. 1998, UK: John Willey & Sons. 294.
17. Kuloor, C. and Eberlein, A. *Aspect-Oriented Requirements Engineering for Software Product Lines*. in *Proceedings of the 10 th IEEE International Conference and Workshop on the Engineering of Computer-Based Systems (ECBS'03)*. 2003.
18. López, F., Amutio, M.A., Candau, J., and Mañas, J.A., *Methodology for Information Systems Risk Analysis and Management*. 2005: Ministry of Public Administration.
19. Mead, N.R. and Stehney, T. *Security Quality Requirements Engineering (SQUARE) Methodology*. in *Software Engineering for Secure Systems (SESS05), ICSE 2005 International Workshop on Requirements for High Assurance Systems*. 2005. St. Louis.
20. Mellado, D., Fernández-Medina, E., and Piattini, M., *A Comparative Study of Proposals for Establishing Security Requirements for the Development of Secure Information Systems*. The 2006 International Conference on Computational Science and its Applications (ICCSA 2006), Springer LNCS 3982, 2006. **3**: p. 1044-1053.
21. Mellado, D., Fernández-Medina, E., and Piattini, M., *A Common Criteria Based Security Requirements Engineering Process for the Development of Secure Information Systems*. Computer Standards and Interfaces, 2007. **29**(2): p. 244 - 253.
22. Mellado, D., Fernández-Medina, E., and Piattini, M., *Aplicando un Proceso de Ingeniería de Requisitos de Seguridad de Dominio para Líneas de Producto Software*. The XI Ibero-American Workshop on Requirements Engineering and Software Environments (IDEAS 2008), 2008: p. 141 - 154.
23. Mellado, D., Fernández-Medina, E., and Piattini, M., *Towards security requriements management for software product lines: a security domain requirements engineering process*. Computer Standards & Interfaces, **(accepted)** (2008). p. http://dx.doi.org/10.1016/j.csi.2008.03.004.
24. Object_Management_Group, *Reusable Assets Specification (RAS)*. 2004, ptc/04-06-06.
25. Pohl, K., Böckle, G., and Linden, F.v.d., *Software Product Line Engineering. Foundations, Principles and Techniques*. 2005, Berlin Heidelberg: Springer.
26. Popp, G., Jürjens, J., Wimmel, G., and Breu, R., *Security-Critical System Development with Extended Use Cases*. 2003: 10th Asia-Pacific Software Engineering Conference. p. 478-487.
27. Schmid, K., Krennrich, K., and Eisenbarth, M., *Requirements Management for Product Lines: A Prototype*. 2005, Fraunhofer IESE.
28. Sindre, G. and Opdahl, A.L., *Eliciting security requirements with misuse cases*. Requirements Engineering 10, 2005. **1**: p. 34-44.
29. Toval, A., Nicolás, J., Moros, B., and García, F., *Requirements Reuse for Improving Information Systems Security: A Practitioner's Approach*. Requirements Engineering, **6**(4) (2002). p. 205-219.


Universidad
de Oviedo

400
cuarto
centenario

PCTI
ASTURIAS

Ayuntamiento de Gijón

GOBIERNO
DE ESPAÑA
MINISTERIO
DE CIENCIA
E INNOVACIÓN

Gobierno del
Principado de Asturias

TIC
CLUSTER ASTURIAS

CSC

INTERSYSTEMS

cajAstur

DEPARTAMENTO DE INFORMÁTICA
UNIVERSIDAD DE OVIEDO

Sistedes
Sociedad de Ingeniería del Software y
Tecnologías de Desarrollo de Software

gijon.info