Computer Standards & Interfaces 30 (2008) 361–371

Contents lists available at ScienceDirect

Computer Standards & Interfaces

journal homepage: www.elsevier.com/locate/csi

Towards security requirements management for software product lines: A security domain requirements engineering process

Daniel Mellado [a,*], Eduardo Fernández-Medina [b], Mario Piattini [b]

[a] Ministry of Work and Social Affairs; Social Security IT Department, Software Development Centre of the National Social Security Institute; Madrid, Spain
[b] ALARCOS Research Group, Information Systems and Technologies Department, University of Castilla-La Mancha, Paseo de la Universidad 4, 13071 Ciudad Real, Spain

ARTICLE INFO

Available online 8 March 2008

Keywords:
Product lines
Common Criteria
ISO/IEC 27001
ISO/IEC 17799
Security requirement
Security requirements engineering
ISMS

ABSTRACT

Security and requirements engineering are one of the most important factors of success in the development of a software product line due to the complexity and extensive nature of them, given that a weakness in security can cause problems throughout the products of a product line. The main contribution of this work is that of providing a security standard-based process for software product line development, which is an add-in of activities in the domain engineering. This process deals with security requirements from the early stages of the product line lifecycle in a systematic and intuitive way especially adapted for product line based development. It is based on the use of the latest security requirements techniques, together with the integration of the Common Criteria (ISO/IEC 15408) and the ISO/IEC 17799 controls into the product line lifecycle. Additionally, it deals with security artefacts variability and traceability, providing us with a Security Core Assets Repository. Moreover, it facilitates the conformance to the most relevant security standards with regard to the management of security requirements, such as ISO/IEC 27001 and ISO/IEC 17799. Finally, we will illustrate our proposed process by describing part of a real case study, as a preliminary validation of it.

1. Introduction

Our society has become increasingly IT-based [34], depending as it does on a huge number of software systems which have a critical role and which manage critical and sensitive information, it is absolutely vital that Information Systems (IS) are properly assured from the very beginning [1,24], due to the potential losses faced by organizations that put their trust in all these IS. Moreover, it is widely-accepted the principle which establishes that the building of security at the early stages of the development process is cost-effective and also brings about more robust designs [18].

Furthermore, nowadays, there is an increase in the demand as well as in the complexity of the software needed. Thus, in order to obtain high-quality IS along with higher productivity, software product line (SPL) based development has become the most successful approach in the reuse field, because it can help us significantly reduce time-to-market as well as development costs [3,4], by increasing the reuse of all types of artefacts, thanks to the combination of coarse-grained components with a top-down systematic approach where software components are integrated into a high-level structure.

Due to the complexity and extensive nature of product line development, security and requirements engineering are much more important for product line practice. Security is a cross-cutting concern in software intensive systems and should consequently be subject to careful requirements analysis and decision making.

In addition the requirements for cost-effective product line development complicate this task. Therefore, the discipline known as Security Requirements Engineering is a very important part of the SPL development process for the achievement of secure SPL and applications/products, because it provides techniques, methods and standards for tackling this task in the development lifecycle. It also implies the use of repeatable and systematic procedures to ensure that the set of requirements obtained is complete, consistent, easy to understand and analysable by the different actors involved in the development of the system [19].

In the last few years, it has been a spectacular growing of security standards and security related proposals which have been developed to try to help develop security critical IS. Moreover, SPL reference architectures for security and SPL requirements management approaches and tools, such as [15,32] have recently been developed. Nevertheless, after analysing the previously performed comparative analyses of several relevant proposals of IS security requirements, as those of [6,23,25,29,31,33,35], etc. in [27,28], we conclude that those standards and proposals are neither specific enough for a systematic and intuitive treatment of SPL security requirements, nor make it easy the task of integrating security requirements engineering activities

* Corresponding author.
E-mail addresses: Daniel.Mellado@uclm.es (D. Mellado), Eduardo.FdezMedina@uclm.es (E. Fernández-Medina), Mario.Piattini@uclm.es (M. Piattini).

0920-5489/$ – see front matter © 2008 Elsevier B.V. All rights reserved.
doi:10.1016/j.csi.2008.03.004

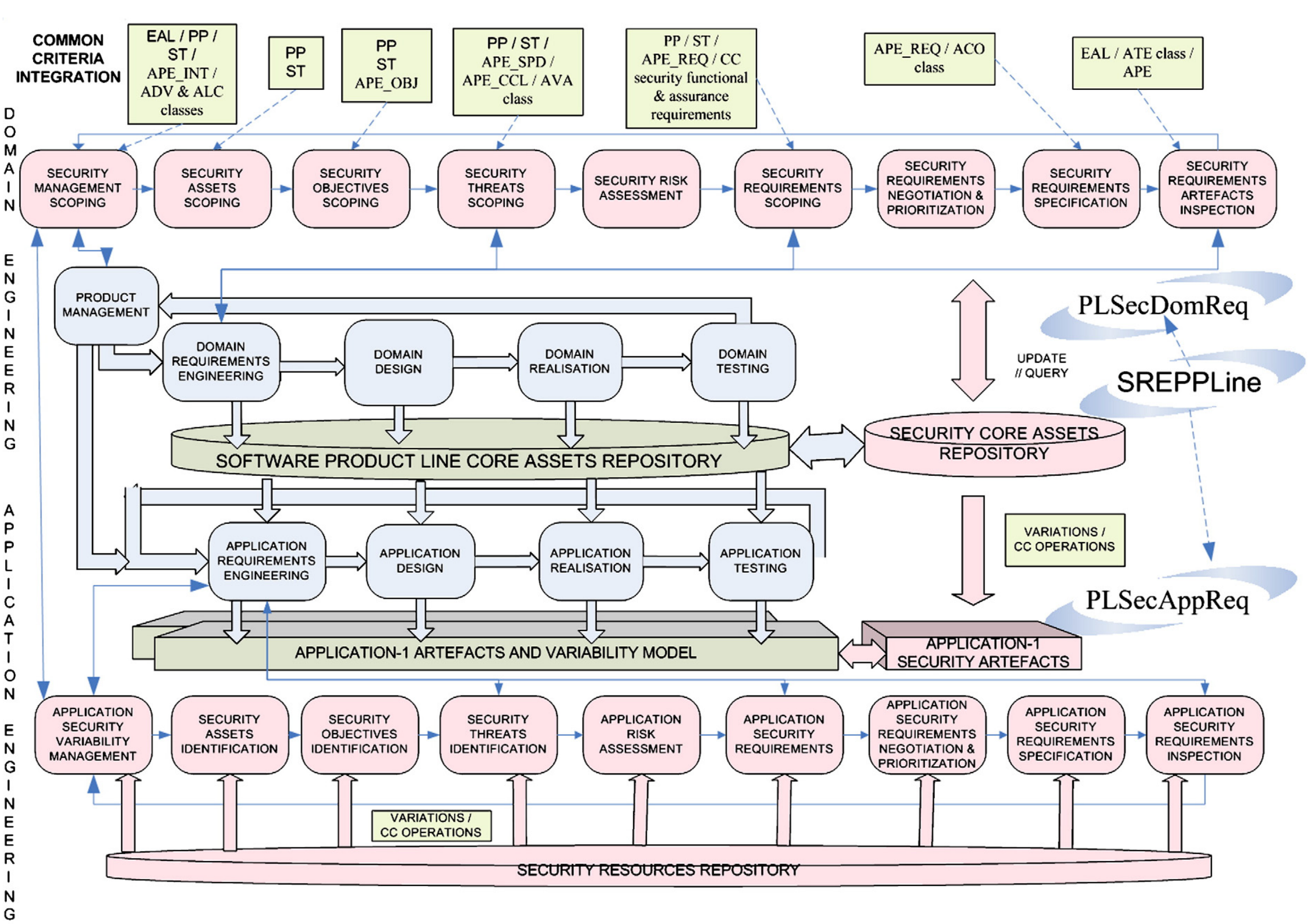
COMMON CRITERIA INTEGRATION
EAL / PP / ST / APE_INT / ADV & ALC classes
PP ST
PP ST APE_OBJ
PP / ST / APE_SPD / APE_CCL / AVA class
PP / ST / APE_REQ / CC security functional & assurance requirements
APE_REQ / ACO class
EAL / ATE class / APE
DOMAIN ENGINEERING
SECURITY MANAGEMENT SCOPING
SECURITY ASSETS SCOPING
SECURITY OBJECTIVES SCOPING
SECURITY THREATS SCOPING
SECURITY RISK ASSESSMENT
SECURITY REQUIREMENTS SCOPING
SECURITY REQUIREMENTS NEGOTIATION & PRIORITIZATION
SECURITY REQUIREMENTS SPECIFICATION
SECURITY REQUIREMENTS ARTEFACTS INSPECTION
PRODUCT MANAGEMENT
DOMAIN REQUIREMENTS ENGINEERING
DOMAIN DESIGN
DOMAIN REALISATION
DOMAIN TESTING
PLSecDomReq
UPDATE // QUERY
SREPPLine
SOFTWARE PRODUCT LINE CORE ASSETS REPOSITORY
SECURITY CORE ASSETS REPOSITORY
APPLICATION ENGINEERING
APPLICATION REQUIREMENTS ENGINEERING
APPLICATION DESIGN
APPLICATION REALISATION
APPLICATION TESTING
VARIATIONS / CC OPERATIONS
PLSecAppReq
APPLICATION-1 ARTEFACTS AND VARIABILITY MODEL
APPLICATION-1 SECURITY ARTEFACTS
APPLICATION SECURITY VARIABILITY MANAGEMENT
SECURITY ASSETS IDENTIFICATION
SECURITY OBJECTIVES IDENTIFICATION
SECURITY THREATS IDENTIFICATION
APPLICATION RISK ASSESSMENT
APPLICATION SECURITY REQUIREMENTS
APPLICATION SECURITY REQUIREMENTS NEGOTIATION & PRIORITIZATION
APPLICATION SECURITY REQUIREMENTS SPECIFICATION
APPLICATION SECURITY REQUIREMENTS INSPECTION
VARIATIONS / CC OPERATIONS
SECURITY RESOURCES REPOSITORY

Fig. 1. Software product line security requirements engineering framework.