Lecture Notes in Business Information Processing

This book constitutes the thoroughly refereed proceedings of seven international workshops held in Stockholm, Sweden, in conjunction with the 27th International Conference on Advanced Information Systems Engineering, CAiSE 2015, in June 2015.

The 38 full and nine short papers were carefully selected from 107 submissions.

The workshops were the Second International Workshop on Advances in Services Design based on the Notion of Capability (ASDENCA), the Third International Workshop on Cognitive Aspects of Information Systems Engineering (COGNISE), the First International Workshop on Digital Business Innovation and the Future Enterprise Information Systems Engineering (DiFenSE), the First International Workshop on Enterprise Modeling (EM), the First Workshop on the Role of Real-World Objects in Business Process Management Systems (RW-BPMS), the 10th International Workshop on Trends in Enterprise Architecture Research (TEAR), and the 5th International Workshop on Information Systems Security Engineering (WISSE).

ISSN 1865-1348

ISBN 978-3-319-19242-0

9 783319 192420

Lecture Notes in Business Information Processing

LNBIP

springer.com

Persson · Stirna (Eds.)

LNBIP 215

Advanced Information Systems Engineering Workshops

CAiSE Workshops 2015

Anne Persson · Janis Stirna (Eds.)

Advanced Information Systems Engineering Workshops

CAiSE 2015 International Workshops
Stockholm, Sweden, June 8–9, 2015
Proceedings

Springer

Lecture Notes in Business Information Processing 215

More information about this series at http://www.springer.com/series/7911

Anne Persson · Janis Stirna (Eds.)

Advanced Information Systems Engineering Workshops

CAiSE 2015 International Workshops
Stockholm, Sweden, June 8–9, 2015
Proceedings

Springer

Editors
Anne Persson
University of Skövde
Skövde
Sweden

Janis Stirna
Stockholm University
Stockholm
Sweden

ISSN 1865-1348 ISSN 1865-1356 (electronic)
Lecture Notes in Business Information Processing
ISBN 978-3-319-19242-0 ISBN 978-3-319-19243-7 (eBook)
DOI 10.1007/978-3-319-19243-7

Library of Congress Control Number: 2015939171

Springer Cham Heidelberg New York Dordrecht London

Printed on acid-free paper

Springer International Publishing AG Switzerland is part of Springer Science+Business Media (www.springer.com)

Preface

The Conference on Advanced information Systems Engineering (CAiSE) has traditionally been focusing on aspects that intersect our field – technological and human, theoretical and application, organizational and societal. CAiSE 2015 focuses on creativity, ability, and integrity in information systems engineering in order to design, develop, and deploy artifacts that can extend the boundaries of human and organizational capabilities. The 27th CAiSE was held in Stockholm, Sweden, June 8–12, 2015.

It has been an established tradition that each year CAiSE is accompanied by a significant number of high-quality workshops. Their aim is to address specific emerging challenges in the field, to facilitate interaction between stakeholders and researchers, to discuss innovative ideas, as well as to present new approaches and tools. This year, CAiSE had two associated working conferences (BPMDS and EMMSAD) and ten workshops. The accepted workshops were chosen after careful consideration, based on maturity and compliance with our usual quality and consistency criteria.

This volume contains the proceedings of the following seven workshops of CAiSE 2015 (in alphabetical order):

- The Second International Workshop on Advances in Services DEsign based on the Notion of CApabiliy (ASDENCA)
- The Third International Workshop on Cognitive Aspects of Information Systems Engineering (COGNISE)
- The First International Workshop on Digital Business Innovation and the Future Enterprise Information Systems Engineering (DiFenSE)
- The First International Workshop on Enterprise Modeling (EM 2015)
- The First Workshop on the Role of Real-World Objects in Business Process Management Systems (RW-BPMS)
- The 10th International Workshop on 'Trends in Enterprise Architecture Research (TEAR)
- The Fifth International Workshop on Information Systems Security Engineering (WISSE)

The 11th International Workshop on Enterprise and Organizational Modeling and Simulation (EOMAS) published post-proceedings in a separate LNBIP volume. The First International iStar Teaching Workshop (iStarT) and the First International Workshop on Socio-Technical Perspective in IS development (STPIS) published their proceedings in the CEUR Workshop Proceedings series. Each workshop adhered to the CAiSE 2015 submission and acceptance guidelines. The paper acceptance rate for the workshops included in these proceedings was approximately 43%.

As workshop chairs of CAiSE 2015 we would like to express our gratitude to all workshop organizers and to all corresponding scientific committees of the workshops for their invaluable contribution.

June 2015

Anne Persson
Janis Stirna

The 2nd International Workshop on Advances in Services DEsign based on the Notion of CApabiliy – ASDENCA 2015

Preface

Lately the notion of *capability* is gaining much presence within the field of Information Systems Engineering, due to a number of factors: the notion directs business investment focus, it can be used as a baseline for business planning, and it leads directly to service specification and design. Historically, it has been examined in Economics, Sociology, and Management Science. More recently, it has been considered in the context of business-IT alignment, in the specification and design of services using business planning as the baseline, in Enterprise Architecture, and in Service Oriented Architecture.

Capability is commonly seen as an *ability* or *capacity* for a company to deliver value, either to customers or shareholders, right beneath the business strategy. It consists of three major components: business processes, people, and physical assets.

Thus it is as an abstraction away from the specifics of how (process), who (agent), and why (goals), i.e. with focus on results and benefits. At the same capability should allow fairly straightforward integrations with the mentioned established bodies of knowledge and practices, such as goals (through "goal fulfillment"), processes (through "modeling"), and services (through "servicing").

The idea for the ASDENCA workshop has come from the academic and industrial community gathered in EU/FP7 project – CaaS. The special theme of the 27th edition of CAiSE was Creativity, Ability, and Integrity in IS Engineering. As systems are moving beyond traditional information management and need to organically blend into the environment appealing to large and diverse user bases, capability orientation in IS design with services may play an important role in novel solutions making use of information from different sources that need to be merged and molded to become meaningful and valuable (creativity), capable to deliver business in excellent, competitive and agile way (ability), as well as in ensuring quality in ethical codes – modifications by authorized parties, or only in authorized ways (integrity).

The Program Committee selected five high-quality papers for the presentation on the workshop, which are included in this proceedings volume. Divided in four sessions, the program of the workshop included two paper sessions reflecting important topics of capability-oriented IS design: modeling, and applications; an invited talk, and a discussion panel.

Patricia Lago	VU University Amsterdam, The Netherlands
Marc M. Lankhorst	BiZZDesign
James Lapalme	École de technologie supérieure, Canada
Christine Legner	University of Lausanne, Switzerland
Peter Loos	IWi at DFKI and Saarland University, Germany
Pericles Loucopoulos	Harokopio University of Athens, Greece
Florian Matthes	Technische Universität München, Germany
Jan Mendling	Wirtschaftsuniversität Wien, Austria
Alexandre Moise	Alithya
Josephine Nabukenya	Makerere University Kampala, Uganda
Agnes Nakakawa	Makerere University Kampala, Uganda
Selmin Nurcan	Université de Paris 1 Panthéon - Sorbonne, France
Andreas L. Opdahl	University of Bergen, Norway
Hervé Panetto	CRAN and University of Lorraine and CNRS, France
Erik Proper	Public Research Centre – Henri Tudor, Luxembourg
Colette Rolland	University of Paris 1 Pantheon-Sorbonne, France
Kurt Sandkuhl	The University of Rostock, Germany
Rainer Schmidt	Munich University of Applied Sciences, Germany
Gerhard Schwabe	Universität Zürich, Switzerland
Christian Schweda	LeanIT42 GmbH, Germany
Ulrike Steffens	HAW Hamburg, Germany
Dirk Stelzer	TU Ilmenau, Germany
Stefan Strecker	University of Hagen, Germany
Pierre-Martin Tardif	Université de Sherbrooke, Canada

Additional Reviewers

Liv Gingnell	Pouya Aleatrati	Margus Välja
Eduardo Loures	Bernhard Waltl	Matus Korman
Timo Kucza	Ovidiu Noran	Timo Kucza
Sinna Lindquist	Ivan Salvador Razo-Zapata	
Björn Pelzer		

The 5th International Workshop on Information Systems Security Engineering – WISSE 2015

Preface

Information systems security problems are currently a widespread and growing concern that covers most of the areas of society, such as business, domestic, financial, government, healthcare, and so on. The scientific community has realized the importance of aligning information systems engineering and security engineering in order to develop more secure information systems. Nevertheless, there is lack of an appropriate event that will promote information systems security within the context of information systems engineering. The proposed workshop fulfills this gap.

The International Workshop on Information System Security Engineering (WISSE) aims to provide a forum for researchers and practitioners to present, discuss, and debate on one hand the latest research work on methods, models, practices, and tools for secure information systems engineering, and on the other hand relevant industrial applications, recurring challenges, problems, and industrial led solutions at the area of secure information systems engineering.

This fifth edition of the workshop, held in Stockholm (Sweden) on June 8th, 2015, was organized in conjunction with the 27th International Conference on Advanced Information Systems Engineering (CAiSE 2015). In order to ensure a high-quality workshop, following an extensive review process, seven submissions were accepted as full papers addressing a large variety of issues related to Secure Information Systems Engineering.

We wish to thank all the contributors to WISSE 2015, in particular the authors who submitted papers and the members of the Program Committee who carefully reviewed them. We express our gratitude to the CAiSE 2015 Workshop Chairs, for their helpful support in preparing the workshop. Finally, we thank our colleagues from the Steering Committee, Jan Jürjens, Haralambos Mouratidis, Carlos Blanco, and Daniel Mellado, and our colleagues from Publicity Chairs, Shareeful Islam, Luis Enrique Sánchez, and Akram Idani, for initiating the workshop and contributing to its organization.

June 2015

Nadira Lammari
David G. Rosado
Christos Kalloniatis

WISSE 2015 Organization

General Chair

Nadira Lammari — Conservatoire National des Arts et Métiers, France

Program Co-chairs

David G. Rosado	University of Castilla-La Mancha, Spain
Christos Kalloniatis	University of the Aegean, Greece

Steering Committee

Jan Jürjens	Technical University of Dortmund, Germany
Nadira Lammari	Conservatoire National des Arts et Métiers, France
Haralambos Mouratidis	University of Brighton, UK
David G. Rosado	University of Castilla-La Mancha, Spain
Carlos Blanco	University of Cantabria, Spain
Christos Kalloniatis	University of the Aegean, Greece

Publicity Chairs

Shareeful Islam	University of East London, UK
Luis Enrique Sánchez	University of Armed Forces, Ecuador
Akram Idani	University of Grenoble, France

Program Committee

Antonio Maña	University of Malaga, Spain
Akram Idani	University of Grenoble, France
Benjamin Nguyen	SMIS, Inria-Rocquencourt, France
Brajendra Panda	University of Arkansas, USA
Bruno Defude	Télécom SudParis, France
Carlos Blanco	University of Cantabria, Spain
Csilla Farkas	University of South Carolina, USA
Daniel Mellado	Spanish Tax Agency, Spain
Djamel Benslimane	LIRIS, Claude Bernard Lyon I University, France
Eduardo Fernández-Medina	University of Castilla-La Mancha, Spain
Eduardo B. Fernández	Florida Atlantic University, USA
El-Bay Bourennane	University of Bourgogne, Dijon, France
Eric Dubois	CRP Henri Tudor, Luxembourg
Ernesto Damiani	Università degli Studi di Milano, Italy
Frédéric Cuppens	Télécom Bretagne, France
Günther Pernul	University of Regensburg, Germany
Guttorm Sindre	Norwegian University of Science and Technology, Norway

Haris Mouratidis	University of Brighton, UK
Hanifa Boucheneb	École Polytechnique de Montréal, Quebec, Canada
Isabelle Comyn-Wattiau	Cnam Paris, France
Jacky Akoka	Cnam Paris, France
Javier López	University of Málaga, Spain
Jan Jürjens	Technical University of Dortmund, Germany
Ludovic Apvrille	Telecom ParisTech, France
Luis Enrique Sánchez	University of Castilla-La Mancha, Spain
Marc Frappier	University of Sherbrooke, Québec, Canada
Marc Chaumont	University of Montpellier, France
Matt Bishop	University of California, USA
Mohammad Zulkernine	Queen's University, Canada
Oliver Popov	Stockholm University, Sweden
Paolo Giorgini	University of Trento, Italy
Régine Laleau	LACL, Université Paris-Est Créteil, France
Sabrina De Capitani di Vimercati	Università degli Studi di Milano, Italy
Shareeful Islam	University of East London, UK
Stefanos Gritzalis	University of the Aegean, Greece
Steven Furnell	Plymouth University, UK
Tristan Allard	University of Montpellier 2, France
Vincent Nicomette	INSA de Toulouse, France
Yves Ledru	LIG, University of Grenoble, France

Contents

DiFenSE 2015

EM 2015

RW-BPMS 2015

TEAR 2015

30. Humberg, T., Wessel, C., Poggenpohl, D., Wenzel, S., Ruhroth, T., J"urjens, j: Using ontologies to analyze compliance requirements of cloud-based processes. In: Helfert, M., Desprez, F., Ferguson, D., Leymann, F. (eds.) CLOSER 2013. CCIS, vol. 453, pp. 1–16. Springer, Heidelberg (2014)
31. Wenzel, S., Wessel, C., Humberg, T., Jürjens, J.: Securing processes for outsourcing into the cloud. In: 2nd International Conference on Cloud Computing and Services Science. SciTePress (2012)

A Framework for Secure Migration Processes of Legacy Systems to the Cloud

Luis Márquez[1(✉)], David G. Rosado[2], Haralambos Mouratidis[3], Daniel Mellado[4], and Eduardo Fernández-Medina[2]

[1] Spanish National Authority for Markets and Competition (CNMC), 28004 Madrid, Spain
luis.marquez@cnmc.es
[2] GSyA Research Group, Department of Information Systems and Technologies, University of Castilla-La Mancha, 13071 Ciudad Real, Spain
{david.grosado,eduardo.fdezmedina}@uclm.es
[3] Secure and Dependable Software Systems (SenSe), University of Brighton, Brighton BN2 4GJ, UK
H.Mouratidis@brighton.ac.uk
[4] Spanish Tax Agency, 28046 Madrid, Spain
damefe@esdebian.org

Abstract. The emergence of cloud computing as a major trend in the IT industry signifies that corporate users of this paradigm are confronted with the challenge of securing their systems in this new environment. An important aspect of that, includes the secure migration of an organization's legacy systems, which run in data centers that are completely controlled by the organization, to a cloud infrastructure, which is managed outside the scope of the client's premises and may even be to-tally off-shore. This paper makes two important contributions. Firstly, it presents a process (SMiLe2Cloud) and a framework that supports secure migration of corporate legacy systems to the cloud. We propose a process based on a continuous improvement cycle that starts with a Knowledge Discovery Meta-Model (KDM) set of models from which a security model for legacy system migration to the cloud is derived. Secondly, it provides a set of clauses (derived from the models) for security cloud providers and custom security cloud controls.

Keywords: Cloud computing · Computer security · Legacy software migration · KDM · CSA

1 Introduction

One of the biggest challenges is defining cloud computing. Based on the Cloud Security Alliance (CSA) [1], cloud computing can be defined as: "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services).

To really understand the level of expectation placed upon cloud computing, one only has to read the recent report published by the European Commission entitled "Unleashing the Potential of Cloud Computing in Europe" [2]. Within this report,

A. Persson and J. Stirna (Eds.): CAiSE 2015 Workshops, LNBIP 215, pp. 507–517, 2015.
DOI: 10.1007/978-3-319-19243-7_46

it anticipates the potential impact of cloud computing could result in "a net gain of 2.5 million new European jobs, and an annual boost of €160 billion to the European Union GDP (around 1 %), by 2020".

Cloud Computing claims to take enterprises search to a new level and allows them to further reduce costs through improved utilization, reduced administration and infrastructure cost and faster deployment cycles [3]. The essence of legacy system migration is to move an existing, operational system to a new platform, retaining the functionality of the legacy system while causing as little disruption to the existing operational and business environment as possible [4]. Legacy system migration is a very expensive procedure which carries a definite risk of failure. Consequently before any decision to migrate is taken, an intensive study should be undertaken to quantify the risk and benefits and fully justify the redevelopment of the legacy system involved [5, 6].

Security plays a recurring concern within multiple end-customer surveys regarding concerns/barriers toward cloud adoption, as do concerns about data privacy. Based on a survey of 489 "business leaders", the PwC report entitled "The Future of IT Outsourcing and Cloud Computing" [7] asked a series of questions to respondents across multiple geographies, industry verticals, and company sizes relating to cloud adoption. When asked about concerns regarding data security, respondents believed it represented the biggest risk to infrastructure in the public cloud. Indeed, 62 % of respondents believed data security as either a serious or an extremely serious risk.

Security consistently raises the most questions as consumers look to move their data and applications to the cloud. Cloud computing does not introduce any security issues that have not already been raised for general IT security. The concern in moving to the cloud is that implementing and enforcing security policies now involves a third party. This loss of control emphasizes the need for transparency from cloud providers [8]. In some cases the cloud will offer a better security posture than an organization could otherwise provide.

There are no initiatives where a migration process is proposed for security aspects [9]. There is an urgent need to provide methodologies, techniques and tools to provide a strategy that facilitate the migration process of security aspects.

Our aim in this paper is to propose a framework, to support secure migration in the cloud, in the form of a set of methods that address the issue of security and how security should be integrated with different kinds of processes in order to migrate legacy information systems to the cloud in [10].

This paper is structured in 2 more sections in addition to this introduction. Section 2 presents the framework and Sect. 3 provides some conclusions and an outline of our future work.

2 SMiLe2Cloud: Process for Security Migration of Legacy Systems to the Cloud

In this section, we propose a process (called as SMiLe2Cloud) for secure Legacy Information Systems (LIS) migration to the cloud model which is, on the one hand, based on the Software Engineering Institute (SEI) horseshoe model [11] and, on the other, on the Deming cycle of continuous improvement. Since we are interested in the

security process itself, and not actually in the general reverse engineering efforts for functional specification, we have supposed that the engineers migrating the LIS have already developed a model that defines the functional specifications and architectural elements of the system (but not the security specifications and security architecture) and that they have documented these specifications and elements in a system that can be converted to a Knowledge Discovery Meta-Model (KDM) specification [12]. It is at this point that we take over and attempt to first to develop the security aspects of the reverse engineered design, and then continue with the rest of the process. We shall define the process by attempting to follow the Software & Systems Process Engineering Metamodel Specification (SPEM) notation as closely as possible.

2.1 Overview

As stated previously, the process starts at the highest point of the horseshoe model once a base security architecture has been obtained and just before the transformation. From there, it continues with the transformation and the refinement of the target system, focusing on specific cloud issues.

The SMiLe2Cloud process consists of five activities addressed by 16 security domains described in [1] and illustrated in Fig. 1. The extraction activity is focused on the use of reverse engineering to extract security issues from LIS to a security model (SMiLe model) defined for our migration process. The second activity is the analysis of the security requirements (SecR), which is based on the extension of the Secure Tropos methodology [13] for the cloud. The design activity is focused on selecting the service model, the deployment model and making the selection of the cloud provider based on CSA Security, Trust & Assurance Registry (STAR) [14]. The deployment activity is focused on developing the deployment specification based on a repository of cloud migration patterns and making the implementation of the system. The fifth activity is the evaluation when a verification and validation of the security model migrated is checked and captures the new security issues to be incorporated into a new cycle of the process and into an analysis of the improvements and changes proposed for our cloud system.

Since KDM lacked specific concerns regarding security issues, part of our process is in fact performed just before a complete reverse engineered specification of the system has been obtained. The extraction activity that is specifically addressed in our process deals with the last part of the reengineering phase of the horseshoe model. Nevertheless, it could be used separately with any security related method aimed at migrating LIS in a secure manner (no matter what the target architecture might be).

2.2 SMiLe2Cloud Activities

In this section we present an in-depth description of the set of activities in our SMiLe2Cloud process shown in Fig. 1. SMiLe2Cloud process has five activities: Extraction, Analysis, Design, Deployment and Evaluation, and a wide set of input and output artifacts for each of the activities that will be described as follows:

Activity 1: Extraction. The extraction is the activity in which the security model for the LIS is derived from the actual code and the technical documentation of the LIS. It is

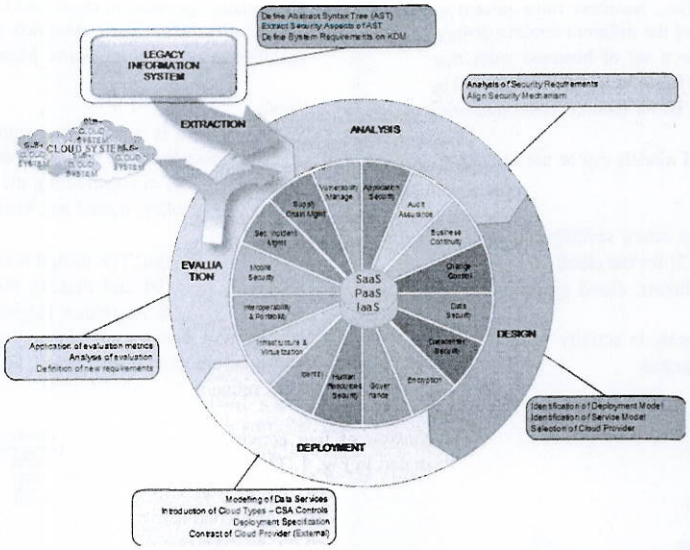

Fig. 1. The SMiLe2Cloud activities

a reverse engineering sub-process that is parallel to the sub-process of obtaining the general architectural model for the LIS. The process is assisted by reverse engineering tools in order to ease the tasks and steps that the analyst must perform to put the different requirements and controls in place.

The process is data oriented and is based on a formal specification of the sub-programs and data managed by each program unit in the LIS in the form of an abstract syntax tree (AST) that models each of the program units.

This activity produces internal artifacts which represent outputs for some tasks and inputs for others. Figure 2 shows a graphical representation of the extraction activity tasks using SPEM 2.0 diagrams.

*A1.*1 Extract Security Aspects

An abstract syntax tree is a tree representation of the syntactic structure of the program and data items of the LIS, and supports a 1-to-1 mapping of all the items included in the code in a tree like structure that is used as the basis to derive the security requirements of the system.

The task has two steps: the first step involves extracting all the information from the LIS by means of traditional reverse engineering techniques (static/dynamic analysis, slicing, etc.) and with the help of tools, while the second step involves defining the AST with the information extracted.

For each data element and each subprogram element that is present in the AST, the system analyst must extract the concrete security permissions that each of the different

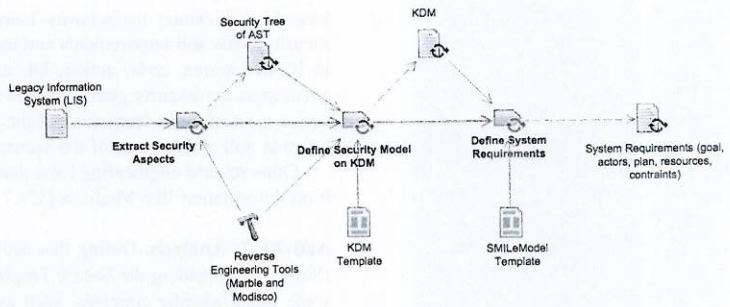

Fig. 2. Extraction activity

user profiles must have to be able to run the program normally (access, create, modify, delete, admin, audit).

*A1.*2 Define security model on KDM

As shown above, as a reengineering meta-model focused on functional specifications, KDM does not have security areas of concern built within the standard itself. Pérez-Castillo [15] state that there are some tools that use KDM to formalize machine-readable content prior to searching for vulnerability patterns and performing the static analysis of the representation of code, but the standard itself does not address the formalization of the security aspects of the LIS. It is true, however, that some of the domains, packages and models defined in the standard are bound to include security references (i.e., business rules domain, data domain, platform, source); but the security references have no single domain, package or model related to security and it is therefore easy for the LIS security requirements and artifacts to end up scattered around the entire collection of models and specifications.

We propose to avoid this situation by ensuring that every single artifact and security control in the LIS is instantiated in a business security rule and is included in the conceptual model during the analysis phase.

*A1.*3 Define system requirements

As described above the extraction activity is focused on the use of reverse engineering to extract security issues from LIS to a security model (SMiLe model) defined for our migration process.

We have at this point our KDM model with particular emphasis on security issues. Based on this model (KDM) we will define the system requirements (SMiLe model) defining the goals, actors, plans, resources and constraints.

The SMiLe model will be implemented as a XML file. This file will be the input for the next activity, the analysis activity.

Tools

In order to assist in this activity we are adapting the reverse engineering tool Marble [16] to support security aspects. We are developing a series of templates with which to

identify and extract the security items in the model (i.e., business rules related to security goals and requirements and assets) from some of the different models defined in KDM (source, code, action, UI, data) and to define a set of business rules that encompass the security goals, policies and requirements for the LIS. We also intend to derive a set of items from most of the other domains of KDM (source, data, platform, UI) that will also be part of the security model.

Other reverse engineering tools that also obtain KDM models can be used to collect more information like Modisco [17].

Activity 2: Analysis. During this activity we define the actual security requirements (SecR), by extending the Secure Tropos methodology [13] for the cloud. We introduce some cloud-specific concepts, such as cloud specific threats, cloud specific security constraints and cloud service providers.

Figure 3 shows a graphical representation of the analysis activity tasks together with the input and output artifacts using SPEM 2.0 diagrams.

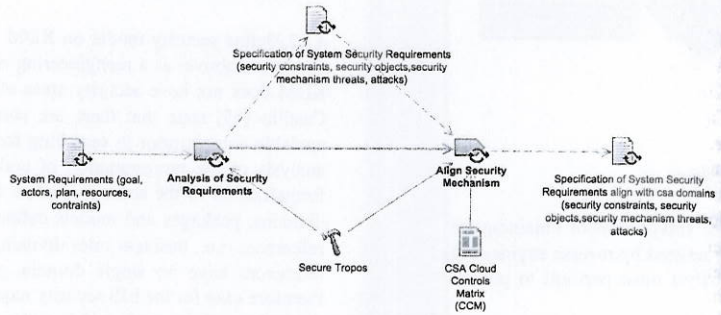

Fig. 3. Analysis activity

A2.1 Analysis of Security Requirements

The SMiLe model is used to derive a set of SecRS with which the system must comply in the new environment.

Two steps are defined in this task: analyze the LIS requirements that are no longer necessary and analyze the new cloud requirements that are applicable.

Some requirements of the original LIS may be no longer applicable to the target system, since the cloud ecosystem might simply have made them redundant or unnecessary. It is also necessary to bear in mind that not all the cloud controls may be applicable to the LIS; an analysis of the applicability of new cloud requirements is therefore necessary before we can proceed further.

A2.2 Align Security Mechanism

The CSA Cloud Control Matrix [18] provides a controls framework in 16 domains that are cross-mapped to other industry-accepted security standards, regulations, and controls frameworks. We have developed a catalogue of security mechanisms based in the

16 domains specified in the Cloud Control Matrix. The objective of this task is to map the security mechanism identified in the previous step (A2.1) with the 16 domains specified in the Cloud Control Matrix using the catalogue of security mechanisms.

Tools

Secure Tropos is a security requirements engineering methodology that considers security throughout the whole development process. SecTro is a tool which assists the security analysts in constructing the relevant Secure Tropos diagrams that are required in order to identify, model and analyze the security issues.

Activity 3: Design. The design activity is focused on selecting the service model, the deployment model and making the selection of the cloud provider based on CSA Security, Trust & Assurance Registry (STAR) [14].

Figure 4 shows a graphical representation of the design activity tasks together with the input and output artifacts using SPEM 2.0 specification.

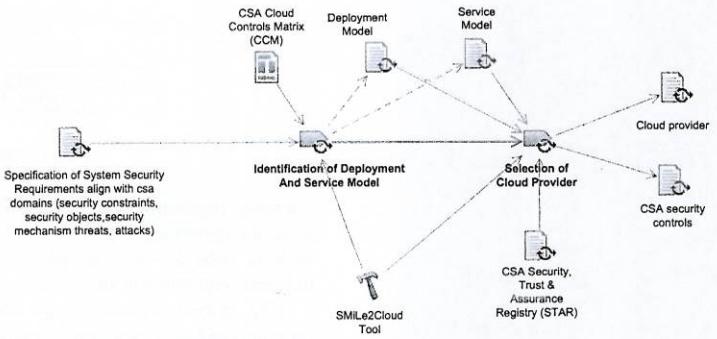

Fig. 4. Design activity

A3.1 Identification of Deployment Model

The National Institute of Standards and Technology (NIST) distinguishes between four cloud deployment models: public, private, hybrid and community.

In this task, based on the specification of system security requirements aligned with the CSA domains we will select the appropriate deployment model for our system.

A3.2 Identification of Service Model

The National Institute of Standards and Technology (NIST) distinguishes between three service models: software as a service (SAAS), platform as a service (PAAS) and infrastructure as a service (IAS).

During this task, based on the specification of system security requirements aligned with the CSA domains, the appropriate service model for our system is defined.

A3.3 Selection of cloud provider
Once we have selected the deployment model, the service model and we have our system security requirements aligned with the CSA domains we can select the cloud providers that fit with our security needs according to the CSA Security, Trust & Assurance Registry (STAR).

Tools
The SMiLe2Cloud Tool helps us throughout the migration process. In the early stages (extraction and analysis) is integrated with the above named tools (Marble, Modisco and SecTro). In the following phases (design, deployment and evaluation) uses its own interface.

Activity 4: Deployment. The deployment activity is focused on developing the deployment specification based on a repository of cloud migration patterns and the implementation of the system.

Figure 5 shows a graphical representation of the migration activity tasks together with the input and output artifacts using SPEM 2.0.

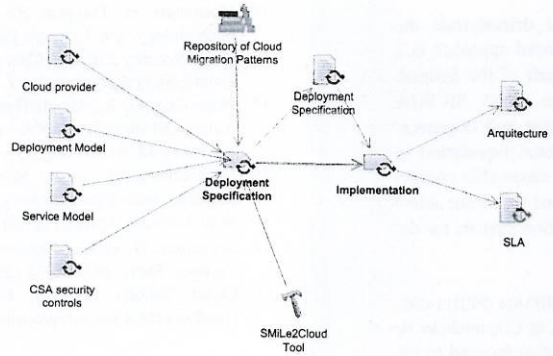

Fig. 5. Deployment activity

A4.1 Deployment Specification
Once we have selected the service model, the deployment model and the cloud provider the deployment specification takes place. This task focuses on the modelling of data services.

A4.2 Implementation
Finally, the implementation itself takes place. During the implementation task it could be necessary to contract the services and to sign the Service Level Agreement (SLA), develop the custom security elements or set all the security controls in working conditions.

Activity 5: Evaluation. Once the entire process has been moved to the cloud in a secure manner, it is time to verify and validate the security of the system. This activity is based on a repository of cloud migration metrics.

Figure 6 shows a graphical representation of the evaluation activity tasks together with the input and output artifacts using SPEM 2.0.

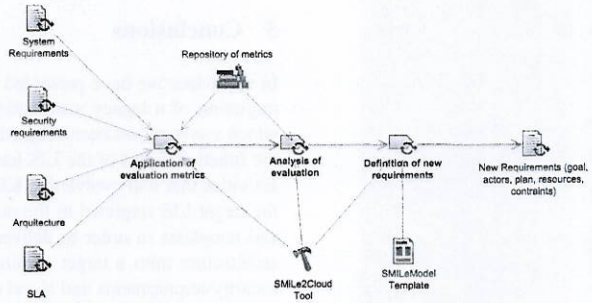

Fig. 6. Evaluation activity

A5.1 Application of evaluation metrics
Despite the obvious value of metrics in different scenarios to evaluate, a formal repository of security metrics in a changing environment like the Cloud is very helpful. In this task, the repository of metrics will be applied to our system.

A5.2 Analysis of evaluation
An analysis of the results obtained in the previous task is necessary. It is necessary to analyze if all the system requirements have been reached, all the security requirements are covered and the architecture is the complete.

A5.3 Definition of new requirements
The cloud is a changing environment. Some of the issues that most experts are now studying were still undetected only a couple of years ago. In two years' time, there might be completely new services that will help to strengthen the security of a LIS system migrated to the cloud. Furthermore, since we have delegated the responsibility for some controls, a continuous watch on the levels and metrics of security is advisable.

Even when the system is operating in working conditions, and as we have already seen, the verification of some parts needs a continuous effort to gather further evidence that the security is maintained at the levels agreed on and that security services are provided.

Activity 5.3 must therefore be periodically repeated, and the results must be analyzed within the limits of the specifications of the security architecture proposed.

But even if the security specifications are met as written, basing our process on a Deming cycle signifies some sort of continuous reevaluation of possible improvements to the system.

The improvements may come from technical advances in the field, from changes in the standard SLA or the services that the cloud provider offers, from legislative grounds, etc.

The new requirements will be implemented as an XML file based in the SMiLe model. This file will be the input for the activity 2, the analysis activity.

3 Conclusions

In this paper we have presented the main stages of a process that supports the secure migration of a legacy information system (LIS) to the cloud. We start at the point at which a system has been subjected to reverse engineering and a KDM set of models for the functional part of the LIS has been extracted. From this point, we propose a set of activities that will evolve that KDM into an LIS security architecture and from there to the target LIS migrated to the cloud; we are currently developing semiautomatic tools and templates in order to deliver a LIS security architecture and to map this security architecture onto a target architecture that specifically addresses cloud threats, cloud security requirements and cloud controls (either as SecaaS or customized controls) that meet cloud security standards such as CSA's controls matrix.

Our future work will focus on improving our process and demonstrate the applicability of the proposed framework. We are applying the proposed approach in a real-world case study based on the migration of the SICILIA system of the Spanish National Authority for Markets and Competition (CNMC) to the cloud. SICILIA manage the liquidation of the special regime installations (renewable and cogeneration). According to the latest report on the results of the provisional liquidation in November 2014 of the remuneration of the production facilities of renewable energy, cogeneration and waste has been cleared a total of 63,878 installations that were active in SICILIA and were entered in the Register of specific Remuneration system for the Ministry of Industry, Energy and Tourism.

Acknowledgments. This research is part of the following projects: SERENIDAD (PEII11-037-7035) financed by the "Viceconsejería de Ciencia y Tecnología de la Junta de Comunidades de Castilla- La Mancha" (Spain) and FEDER, and SIGMA-CC (TIN2012-36904) financed by the "Ministerio de Economía y Competitividad" (Spain).

References

1. Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing V3.0 (2011)
2. European Commission, Unleashing the Potential of Cloud Computing in Europe. Communication from the commission to the European Parliament, the council, the European economic and social Committee and the Committee of the regions (2012)
3. Kushwah, V.S., Saxena, A.: A security approach for data migration in cloud computing. Int. J. Sci. Res. Publ. **3**(5) (2013)

4. Wu, B., et al.: Legacy system migration: a legacy data migration engine. In: 17th International Database Conference (DATASEM 1997), pp. 129–138. Czech Republic, Brno (1997)
5. Bisbal, J., et al.: Legacy information system migration: a brief review of problems. Solutions Res. Issues **16**(5), 103–111 (1999)
6. Bisbal, J., Lawless, D., Richardson, R.: A Survey of Research into Legacy System Migration. Computer Science Department, Trinity College Dublin (1997)
7. PwC, The Future of IT Outsourcing and Cloud Computing (2011)
8. Cloud Computing Use Case Discussion Group, Cloud Computing Use Cases White Paper version 4.0 (2010)
9. Alcañiz, L.M., et al.: Security in legacy systems migration to the cloud: a systematic mapping study. In: 11th International Workshop on Security in Information Systems, pp. 93–100. Lisbon, Portugal (2014)
10. Rosado, D.G., et al.: Security analysis in the migration to cloud environments. Future Internet **4**, 469–487 (2012)
11. Seacord, R., Plakosh, D., Lewis, G. (eds.): Modernizing Legacy Systems: Software Technologies, Engineering Processes, and Business Practices, Addison-Wesley Professional, p. 352 (2003)
12. OMG, Architecture-Driven Modernization. Knowledge Discovery Meta-Model (KDM), v1.3 (2011)
13. Mouratidis, H., Giorgini, P.: Secure tropos: a security-oriented extension of the tropos methodology. Int. J. Softw. Eng. Knowl. Eng. **17**(2), 285–309 (2007)
14. Cloud Security Alliance. CSA Security, Trust & Assurance Registry (STAR) (2014). https://cloudsecurityalliance.org/star/
15. Pérez-Castillo, R., García-Rodríguez de Guzmán, I., Piattini, M.: Knowledge discovery metamodel-ISO/IEC 19506: a standard to modernize legacy systems. Comput. Stand. Interfaces **33**, 519–532 (2011)
16. Pérez-Castillo, R., et al.: MARBLE: a modernization approach for recovering business processes from legacy systems. In: International Workshop on Reverse Engineering Models from Software Artifacts (REM 2009) (2009)
17. Bruneliere, H., et al.: Modisco: a model driven reverse engineering framework. Inf. Softw. Technol. **56**(8), 1012–1032 (2014)
18. Cloud Security Alliance. CLOUD CONTROLS MATRIX V3.0.1 (2014). https://cloudsecurityalliance.org/download/cloud-controls-matrix-v3-0-1/