Using Security Patterns to Tailor Software Process

Rosana Wagner
Instituto Federal Farroupilha
Alegrete, Brasil
rosanawagner@gmail.com

Lisandra Manzoni Fontoura
Universidade Federal de Santa Maria
Santa Maria, Brasil
lisandramf@gmail.com

Adriano Brum Fontoura
Instituto Federal Farroupilha
Santo Augusto, Brasil
afontoura@sa.iffarroupilha.edu.br

Abstract — Secure software development processes can reduce the quantity of security errors and the vulnerabilities involved in software projects. A secure development process is composed by activities that propose the insertion of security requirements in all software development phases. These activities can be based on standards and/or security models such as SSE-CMM, ISO/IEC 27001, ISO/IEC 15408. The problem is that the standards and security models describe security requirements which can be followed but do not describe how these requirements must be implemented in software processes. Security patterns describe good security practices which can be incorporated to the software process and satisfy the requirements that are described by the standards and models. This work proposes a methodology for the tailoring of software processes based on security requirements that are defined by the security practices of the Systems Security Engineering Capability Maturity Model (SSE-CMM). The tailoring has as basis a process framework that is elaborated from the Rational Unified Process (RUP) and security patterns proposed on the literature.

Keywords - software processes, information security, processes tailoring, security patterns.

I. INTRODUCTION

The lack of security in software projects is one of the main concerns of the organizations. It is through the vulnerabilities that are present in software projects that the secrecy breaking and the information theft occur. Due to this factor, the organizations are seeking to adopt measurements that are more and more rigorous in terms of protection aligned with standards and security models [1].

The SSE-CMM model (System Security Engineering Capability Maturity Model) [2], currently known as the ISO/IEC 21827 standard, provides a set of good security practices which can be adopted by the organizations in order to increase the software security. The model is recommended for the development of secure software and the elaboration of security management processes.

The security patterns provide solutions that are already consolidated for recurrent problems and serve as reference for the organizations that seek to satisfy security requirements [3]. Thus, patterns can be associated to the SSE-CMM practices, identifying how they may be incorporated into a software process. The incorporation of the patterns into the software process happens at the moment of the process tailoring to answer to the specific needs of a project.

This article proposes an approach to processes tailoring that have as basis a process framework which is built from the Rational Unified Process and from security patterns association rules to the SSE-CMM process areas. The processes that are obtained from the framework aim at the development of secure software.

Tailoring processes consists in altering or adapting the descriptions of a process for a particular purpose. In this article, the tailoring is given by means of selecting and incorporating patterns into organization’s software process, which is instantiated from the framework, originating the specific software process to use in a project. A methodology for processes tailoring that is based on the framework is proposed.

The contributions of this work include the methodology proposal for software processes tailoring based on security requirements, the framework for elaborating secure processes, which can be customized by the user, and a tailoring support tool.

II. SOFTWARE PROCESS SECURITY

Elaborating secure processes can be obtained by means of the security patterns incorporation, which describe consolidated solutions for recurrent security problems, that are associated to the practices of the SSE-CMM Model.

The System Security Engineering Capability Maturity Model (SSE-CMM) describes the essential characteristics that must exist in the processes of an organization in order to assure a good systems security by means of 22 process areas (PAs) that are organized in two groups: Security Base Practices and Organizational and Project Base Practices. In this work we considered the Security Base Practices because they are responsible for implementing security in software processes, which is the objective of this work.
Security patterns have been associated to security base practices because they provide solutions for recurrent security problems. The patterns capture the experience of security specialist individuals and provide solutions for security related problems which can be applied by non-specialist individuals. Associating security patterns to the base practices facilitate the processes tailoring, since once the association rules are defined it is not necessary that the process engineer is a security specialist.

The solution that is proposed by a pattern can be implemented with the help of other patterns, which solve parts of the whole problem [4]. The most known pattern catalogues are: Schumacher et al. [3], Rosado [5], Romanosky [7], Kienzle and Elder [8].

III. ELABORATING THE SECURITY METHODOLOGY TAILORING (SMT) FRAMEWORK

The processes tailoring that is proposed by this work is based on a process framework elaborated from Rational Unified Process. This framework is extended by adding a set of security related activities. The security related activities aims to satisfy the PAs of the SSE-CMM and have been defined from security patterns catalogues [3][5][7][8][9][10]. It is important to highlight that new activities can be added to the proposed framework according to the organization necessities.

The process for elaborating the SMT framework followed the undermentioned stages: elaborating rules to associate process areas to security patterns and incorporating these rules, security patterns and process areas to the framework.

A. Elaborating the Association Rules

Considering that the PAs have a list of objectives that indicate the expected results after its implementation and a list of BPs (Base Practices) that assist in the making of the objectives, the systematics followed to identify the patterns was the undermentioned: based on the objectives of the PA and its BPs, we have analyzed pattern catalogues to search for patterns, one or more, that addressed to these objectives. Examples provided in the PA description were also considered.

The association of each PA to the patterns that satisfy their objectives originates an association rule. As an example of an elaborate rule, we quote the usage of the Asset Valuation [4]; Threat Assessment [4]; Vulnerability Assessment [4] and Risk Determination [4] patterns for implementing PA03 – Assess Security Risk.

The purpose of Assess Security Risk is to identify the security risks involved with relying on a system in a defined environment. This process area focuses on ascertaining these risks based on an established understanding of how capabilities and assets are vulnerable to threats. Specifically, this activity involves identifying and the assessing the likelihood of the occurrence of risk exposures. The risk assessment is made in order to support the decisions related to the development, maintenance or system operation whose environment is known.

Table I shows the rules of association to the process areas that are elaborated in this work.

<table>
<thead>
<tr>
<th>Process Areas</th>
<th>SuggestedPatterns</th>
</tr>
</thead>
<tbody>
<tr>
<td>PA01 – Administer Security Controls</td>
<td>Security Provider [7]; Controlled Process Creator [3]; Access Control Requirements [3]; Role Rights Definition [3]; Role Based Access Control [3]; Authorization Pattern [5]; Multilevel Security Pattern [5];</td>
</tr>
<tr>
<td>PA02 – Assess Impact</td>
<td>Risk Determination [3];</td>
</tr>
<tr>
<td>PA03 – Assess Security Risks</td>
<td>Asset Valuation [3]; Threat Assessment [3]; Vulnerability Assessment [3]; Risk Determination [3];</td>
</tr>
<tr>
<td>PA04 – Assess Threats</td>
<td>Threat Assessment [3];</td>
</tr>
<tr>
<td>PA05 – Assess Vulnerabilities</td>
<td>Vulnerability Assessment [3];</td>
</tr>
<tr>
<td>PA06 – Build Assurance Argument</td>
<td>Patch Proactively [8]; Engage Customers [9]; Check Point [10]; Red Team the Design [8];</td>
</tr>
<tr>
<td>PA07 – Coordinate Security</td>
<td>Enterprise Partner Communication [3]; Share Responsibility for Security [8]; Gatekeeper [9]; Buffalo Mountain (organizational) [9];</td>
</tr>
<tr>
<td>PA08 – Monitor Security Posture</td>
<td>Minefield [8]; Security Accounting Requirements [3]; Security Accounting Design [3]; Audit Requirements [3]; Audit Design [3]; Audit Trails &amp; Logging Requirements [3]; Audit Trails &amp; Logging Design [3]; Non-Repudiation Requirements [3]; Non-Repudiation Design [3];</td>
</tr>
<tr>
<td>PA10 – Specify Security Needs</td>
<td>Security needs Identification for Enterprise Assets [3];</td>
</tr>
</tbody>
</table>

The rules of association pattern to process areas are suggestions elaborated through the literature and may be improved by the organization by analyzing past projects, retrospective sessions, etc.

B. Incorporating the Association Rules to the Framework

After defining the association rules, it is necessary to incorporate them to the framework, as well as their constituent elements (security patterns and process areas).
So that security patterns may be incorporated into software processes, it is necessary that they are described by means of concepts that will be used in the processes modeling. Metamodels are used to describe elements that can be used for the process elaboration. In this work, we have decided to use the PRiMA-M (Project Risk Management Approach – Metamodel) metamodel (Fig. 1), which was elaborated in previous works by one of the authors [12]. PRiMA-M represents a set of concepts that are used to elaborate software processes. Process elements, instantiated from the PRiMA-M, can be used in the definition of planned, agile or hybrid processes.

This metamodel was elaborated from the concepts described in the Rational Unified Process. The following is an explanation about the classes of this metamodel. More information can be obtained in [12][13].

Lifecycle of a process is an aggregation of Phases which, in turn, are associated to Activities. A Discipline identifies a set of Workers which participate in the Discipline and define a set of Activities that compose the Discipline. An Activity specifies a particular collaboration within a Discipline and represents Tasks grouping, given that a Worker is responsible for each Task.

Artifacts are products generated during the execution of Tasks and may be models, plans, software versions, reports, etc. Workers represent the roles executed by individuals in a project. Tools are used to assist the making of tasks. ToolsMentors describe how to execute a Task by using a certain Tool.

In order to exemplify how security patterns can be described by means of process elements, instantiated from the PRiMA-M, the Asset Valuation pattern, described by using the process elements proposed in the framework, can be visualized in the Fig. 2.

Figure 1. PRiMA – Metamodel adapted from [12][13]

Figure 2. Asset Valuation pattern represented by using process elements proposed in PRiMA-M

The security engineer executes the tasks with the assistance of the project manager. The main artifact elaborated during the execution of these tasks is the Security Requirements document which describes the assets along with the security value, financing value and the impact that the asset may have in the business, as well as the assessment tables that were elaborated for the asset assessment.

Each pattern that is described in an association rule has been defined by using the process elements proposed in the metamodel. The execution sequence of the activities has been defined by means of an activity diagram proposed by the UML. In the RUP, activity diagrams are proposed for each discipline in order to organize the activities that are possible to be executed in the software processes instantiated from it.

Considering that disciplines in the RUP seek to group activity collections related to a concentration area, we opted to group the proposed activities in order to add security to the RUP in one single discipline, named “Software Security”. Another alternative would be to set activities related to security in the existing disciplines in the Unified Process, for example, “Specify Security Needs” could be inserted to the Requirements discipline. Several disciplines would have their activity diagrams altered, which makes difficult for the understanding and implementation of the process. Another advantage of having a separate discipline for dealing with security issues is the facility that organizations will have if they wish to extend their process based on this work.

This discipline has been elaborated according to the orientations for tailoring of the RUP [5], and it must be executed in all phases but with more intensity in the inception and elaboration phase. Considering that, supporting disciplines are concerned with the overall management and structure of a RUP project, Software Security is this type because it concerns security management.
Each activity proposed for patterns implementation has been analyzed in order to define the activity execution sequence. This sequence has been defined from analyzing artifacts that are necessary to the activity execution and artifacts that were generated by activities. The sequenced activities have been organized in an activities diagram for the security discipline (Fig. 3).

IV. METHODOLOGY PROPOSED FOR TAILORING

The methodology for software processes tailoring has the objective of allowing the elaboration of a software development process for a specific project, considering security practices that are described in the SSE-CMM and the SMT framework that is described in the section III.

In this work, the processes tailoring considers that there is an organization’s standard software process (OSSP), which describes the process elements that must exist in all projects of the organization. The tailoring consists in altering OSSP in order to satisfy the project needs, especially in relation to security, and it results in the project-specific process (PSP). Fig. 4 shows the activities proposed methodology.

The patterns that seek to satisfy the PAs are selected based on the association rules defined in the SMT framework. The process engineer selects the patterns that they wish to incorporate to the OSSP from the suggested list. After selecting the security patterns, the process elements associated to their implementation are incorporated to the OSSP originating the PSP.

V. SMT – TOOL

An experimental environment to processes tailoring based on security requirements was developed and it is composed by the tools: Security-Based Methodology Tailoring (SMT-TOOL), Project Risk Management Approach (PRIMA-TOOL) [12] and Pattern-Based Methodology Tailoring (PMT-TOOL) [15].

PMT-Tool is responsible for cataloguing the security patterns. SMT-Tool is responsible for registering the processes areas and associates them to the security patterns. PRIMA-Tool module is responsible for the elaboration of the project software process, from organization’s standard process tailoring, inserting in it the elements of the process associated to the selected patterns to the satisfaction of the processes areas proposed by SSE-CMM.

Having concluded the project process tailoring, PRIMA-Tool generates a website with the description of the project-specific software process to be consulted by developers, managers and process engineers. The website facilities easier the adoption of the software process by the developing team. These tools were used for the achievement of the case studies.

VI. CASE STUDIES

Two case studies were carried out to validate the proposed methodology. The first case study was made on XirooPACS system from Animati Computação Aplicada enterprise.

XirooPACS is a system about filing and communication of medical images. Examinations scheduling, patients’ registers and the appraisal delivering of doctors and patients ordering by the internet are the main features of this system.

The second case study was made on Plex system, from Elevata enterprise. PLEX is a credit card system which aims to enable the enterprises to have their own credit cards. This system joins services of cards administration including monitored selling services and evaluated risks.

The entry to PLEX system is made on web. As the data bases of this system will involve data of many clients and several enterprises, and also flaws may cause a huge financial loss, this is a system which needs a high level of security involved in the process. The system analysis was made considering mainly the data bases and the integration on clients register and charge.

For the study case realization was used SMT framework proposed by this work. In the database of tools was inserted the elements of the process recommended by Rational Unified
Process, as well as the rules of association presented on Table I. Each pattern associated to a process area was described using the process elements proposed by the metamodel.

The first step in the realization of the case study was the filling of a questionnaire to the identification of the process area necessary for each project. The questionnaire was distributed to the project manager who with his team, answered the questionnaire for the prioritization of the security requirements (process areas) proposed by SSE-CMM model. The questionnaire contains the needs specifications to the understanding of the process areas. It was used a scale of relevance to the following levels: highest, high, medium, low or not relevant. The project manager attributed a level to each process area.

Based on the answers and on the framework configured on the tools the processes were adapted and are analyzed on next section.

A. Case Studies Analysis

The developed studies generated project-specific software process to each of the systems. These processes are used as a guide to the project development.

The case studies were made with projects which have very distinct features, although both of them need a high security level and therefore, generate specific-process similar. At the first case study, some process areas were not prioritized for the project security, yet on the second case study all the process areas were considered high or highest to the project, all of these prioritized (Table II).

The verification of whose activities are really high important to the project is not an easy task, once the consideration of adding requirements, which are not really necessary, it can be added extra and unnecessary costs to the project.

Through the two case studies was possible to verify the second project demands more security because the security engineer assigned to all process areas a high or highest importance. More preoccupation related to assess threads and vulnerabilities, build assurance argument, coordinate security and monitor security posture were presented; corresponding to process areas which were not implemented at the first study.

<table>
<thead>
<tr>
<th>PROCESS AREAS</th>
<th>XIROOPACS</th>
<th>PLEX</th>
</tr>
</thead>
<tbody>
<tr>
<td>PA01 – Administer Security Controls</td>
<td>High</td>
<td>Highest</td>
</tr>
<tr>
<td>PA02 – Assess Impact</td>
<td>High</td>
<td>Highest</td>
</tr>
<tr>
<td>PA03 – Assess Security Risks</td>
<td>High</td>
<td>Highest</td>
</tr>
<tr>
<td>PA04 – Assess Threats</td>
<td>Medium</td>
<td>High</td>
</tr>
<tr>
<td>PA05 – Assess Vulnerabilities</td>
<td>Medium</td>
<td>Highest</td>
</tr>
<tr>
<td>PA06 – Build Assurance Argument</td>
<td>Low</td>
<td>Highest</td>
</tr>
<tr>
<td>PA07 – Coordinate Security</td>
<td>Medium</td>
<td>High</td>
</tr>
<tr>
<td>PA08 – Monitor Security Posture</td>
<td>Medium</td>
<td>Highest</td>
</tr>
<tr>
<td>PA09 – Provide Security Input</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>PA10 – Specify Security Needs</td>
<td>Highest</td>
<td>High</td>
</tr>
<tr>
<td>PA11 – Verify and Validate Security</td>
<td>High</td>
<td>Highest</td>
</tr>
</tbody>
</table>

The generated processes as the tailoring result were evaluated jointly to the project managers who on their analyses described that the process tailored to security presents clear activities to be implemented.

The rules of pattern association to the process areas are suggestions elaborated through the literature and may be improved by the organization by analyzing past projects, retrospective sessions, etc.

VII. RELATED WORKS

The development of reliable software has been discussed on many works which seek ways of enhancing the assurances of a project security or a software process. Some related works are presented next.

Mellado, Mediana and Piattini consider security requirements since the initial level of development of production lines, through an interactive and incremental process which where can be added additional tasks, according necessities. Through this tasks incorporation these authors search to make easier the conformity with the security requirements and manage the possible varities which can happen on security requirements. The authors do not exemplify how the security requirements, out of security rules can be unfolded into task. In this sense, this article aims to define the tasks from the patterns association, which, usually, are widely explained or even suggest the tasks to be realized to fulfill the associated requirement.

Paes and Hirata (2007) propose an extension to the RUP with the inclusion of a discipline called "security". The discipline is based on good-practices and on experiences of the authors [5], but does not consider security standards or models. It is not described on this work how the defined process can be tailored to the projects needs.

Hafiz, Adamczyk and Johnson (2007) aim on using patterns to meet the criteria of security software. Although, the authors relate that there is a huge numbers of available security patterns and it is hard to choose which pattern is more recommended to each situation, as well as how to organize them to be used in a project.

This work is different from the others because it proposes a tailoring of software processes using security patterns and also because it elaborates a framework to make easier the elaboration of secures processes. The utilization of practices recommended by SSE-CMM model and of security patterns aim to use practices already consolidated for the development of reliable software.

VIII. CONCLUSIONS

This work proposes a methodology for processes tailoring that considers security requirements, which are proposed by a security model as criterion for tailoring, generating reliable software processes.

Information security has shown itself to be more and more important for the organizations, developers and users, and considering security from the beginning of the software development is desirable.
Elaborating a methodology for software processes tailoring is important to ease the tailoring task. The efficiency of the processes elaborated from the framework will depend on the rules of association pattern to process areas. An initial framework has been elaborated from the Rational Unified Process and activities proposed by the literature; from the security requirements proposed by the SSE-CMM and by the ISO/IEC 27001 Standard; and from security patterns described by Schumacher et al. [4], Rosado [5], Romanosky [7], Kienzle, among others.

The framework proposes a way to organize different elements used to elaborate new process. The organization can define patterns, processes elements and association rules that are adequate to their reality. The framework can be updated and must improve with time and as the team gets more experience. Results of post-mortem analysis of projects can help in this task.

Future work includes the definition of criterion associated to the security rules that seek to facilitate the prioritization of patterns to be applied in determined context and the experimentation of processes tailored by SMT in real projects.

ACKNOWLEDGMENT

We want to express our gratitude to CAPES (Coordenação de Aperfeiçoamento de Pessoal de Nível Superior) for the financial support and a special gratitude to the organizations Animati and Elevata and their projects managers Jean Carlo Albiero Berni and Marcio Puntel for all their feedback and the very useful scientific discussions.

REFERENCES


