Journal of Universal Computer Science, vol. 18, no. 12 (2012), 1608-1627
submitted: 15/9/11, accepted: 15/2/12, appeared: 28/6/12 © J.UCS

Aligning Security and Privacy to Support the Development of Secure Information Systems

Haralambos Mouratidis
(School of Architecture, Computing, and Engineering, University of East London, UK
haris@uel.ac.uk)

Christos Kalloniatis
(Cultural Informatics Laboratory, Dept. of Cultural Technology and Communication
University of the Aegean, Mytilene, Greece
chkallon@aegean.gr)

Shareeful Islam
(School of Architecture, Computing, and Engineering, University of East London, UK
shareeful@uel.ac.uk)

Marc-Philippe Huget
(LISTIC/ Polytech Annecy-Chambéry, University of Savoie, Annecy-Chambéry, France
Marc-Philippe.Huget@univ-savoie.fr)

Stefanos Gritzalis
(Laboratory of Information and Communication Systems Security, Dept. of Information and Communications Systems Engineering, University of the Aegean, Mytilene, Greece
sgritz@aegean.gr)

Abstract: The increasing dependency on information systems to process and manage sensitive information requires the usage of development methods that support the development of secure and private information systems. The literature provides examples of methods that focus on security and privacy individually but fail to provide evidence of information systems development methods that consider security and privacy in a unified framework. Security and privacy are very much related, in particular certain security properties and mechanisms support the achievement of privacy goals. Without a development framework to support developers to explicitly model that relationship, conflicts and vulnerabilities can be introduced to a system design that might endanger its security. In this paper, we present our work in developing a framework that supports the unified analysis of privacy and security. In particular, we present a meta-model that combines concepts from security and privacy requirements methods, such as security and privacy goals, properties, constraints, and actor and process patterns within a social context. A real case study is employed to demonstrate the applicability of our work.

Keywords: Security, privacy, constraints, goal modelling, meta-model
Categories: D.2.1, D.2.2, H.1, K.6.5

1 Introduction

Security and privacy issues become increasingly important for software systems that process and manage critical business and user needs. Every asset needs to be protected so that attackers must not gain unauthorised access, by any means, to a resource. As such, research efforts in the areas of security and privacy have been increased the last few decades. The last few years, both the research and the industrial communities have argued about the need to consider security and privacy in a proactive manner, and develop software engineering techniques that incorporate security and privacy analysis from the early stages of the system development [Mouratidis, 06]. In fact, the literature provides numerous examples of software engineering techniques that assist the elicitation and analysis of security and privacy issues at the requirements stage [Massey, 09],[Kalloniatis, 08], [Sindre, 05], [Mouratidis, 06], [Mead, 06]. However, most of these efforts focus individually on either security or privacy and the literature fails to provide evidence of work that supports the analysis of those two concepts in a unified framework.

Recent research efforts on privacy fall into two main categories: security-oriented requirement engineering (SRE) methodologies [Moffett, 95],[He, 03],[Houmb, 10] and privacy enhancing technologies (PETs) [Massey, 09], [Kalloniatis, 08], [Jensen, 05],[Koorn, 04]. The former focuses on methods and techniques for considering security issues (including privacy) during the early stages of a system development and the latter describes technological solutions for assuring user privacy during system implementation. Also, most of the security-oriented methodologies treat privacy as a subset of security and specifically as one of the security requirements that a system should meet. However, latest research efforts [Cannon, 04], [Koorn, 04], [Fischer-Hübner, 01] have identified that privacy should be treated separately as a separate requirement criterion since privacy itself is a multifaceted concept but not independent from security and vice-versa. Thus the need to analyse security and privacy separately but under a unified framework is of vital importance.

The original contribution of this paper is a meta-model that supports the simultaneous analysis of security and privacy concerns. The presented meta-model defines security and privacy concepts along with requirements engineering concepts. The paper employs a real case study, based on the University of the Aegean Career Office system, to illustrate the meta-model. Our work is part of a greater effort to develop secure and private software systems, based on the application of model-based security and privacy techniques.

2 The need to consider Security and Privacy under a unified framework

Recent literature on security and privacy provides a number of methods for dealing with the elicitation and realisation of security and privacy requirements. However, a general observation of the impact of these methods is that none deals with the security and privacy issues holistically from the elicitation stage through the implementation stage. In fact, the literature presents methods that focus on either security issues or privacy issues individually, while when a method attempts to deal with both issues, it either presents privacy as a subset of security requirements' set or the opposite. However, as recent research imposes [Kalloniatis, 08], [Kavakli, 07], [Cannon, 04], [Fischer-Hübner, 01] privacy itself is a multifaceted concept. Review of current research, highlights the path for user privacy protection in terms of eight privacy requirements namely, authentication, authorization, identification, data protection, anonymity, pseudonymity, unlinkability and unobservability [Cannon, 04], [Koorn, 04], [Fischer-Hübner, 01]. The first three requirements are basically security requirements but they are included due to their key role in the privacy protection. Addressing these requirements is of vital importance when one aims to minimize or eliminate the collection of user identifiable data. Based on the complexity of privacy, it is obvious that it should be dealt as a separate requirements criterion but not independently since the realisation of privacy may affect security and vice-versa. Thus, providing a framework that analyses these two complex concepts and examines their impact on business goals and processes ending with the proper suggestion of appropriate implementation techniques eliminates the gap that exists today as described above.

Another significant fact that leads to the creation of a unified framework is the way that recent methods attempt to implement security and privacy. Specifically, most methods don’t examine the interaction between security and privacy from the requirements level and the impact of this interaction on the rest of the system under development. Their main focus is on the implementation phase and which software tools best realise and implement most of the issues identified. Focusing on the later stages of the development process for addressing either security or privacy is not effective and efficient and hinders the proper realisation of these concepts. The main reason for this inefficiency is the amputation of the organisation’s knowledge in the selection of the appropriate implementation techniques. If security and privacy are not dealt from the early stages of system development in order to understand their role and impact on the achievement of the organisation’s goals being set, developers will end up choosing/developing inappropriate implementation techniques that will not fit exactly on the organisational needs. A number of methods have attempted to connect security requirements with implementation techniques and privacy requirements respectively. But the main challenge today is how to implement both security and privacy together from the elicitation phase through the implementation phase because it has been noted that security and privacy are sometimes overlapping, supplementing or conflicting. The successful analysis of security and privacy individually does not necessarily lead to the successful cooperation of these two requirements.

For better understanding the challenges presented today a comparison of the most well-known methods that deal with security and privacy based on our previous work [Kalloniatis, 09] is presented in Table 1. Specifically, ten methods, were compared based on a four views comparison framework expressed by the following questions: in which stage of the Requirements Engineering (RE) process are the methods applied (usage view); what type of security and privacy issues do they address (subject view); what mechanisms do they offer for expressing security and privacy issues (representation view); what kind of support do they provide to designers in applying proposed way-of-working (development view). The methods selected were the following:

- The NFR (Non-Functional Requirement Framework) method [Chung, 93]
- The i* method [Yu, 93]
- The Tropos method [Mouratidis, 07a]
- The KAOS method [Letier, 00]
- The GBRAM (Goal-Based Requirements Analysis Method) method [Antón, 00]

- The RBAC (Role-Based Access Control) method [He, 03]
- The M-N (Moffett-Nuseibeh Framework) method [Moffett, 95]
- The B-S (Bellotti-Sellen Framework) method [Bellotti, 93]
- The STRAP (STRuctured Analysis for Privacy) method [Jensen, 05]
- The PriS (Privacy Safeguard) method [Kalloniatis, 08]

A detailed description of the aforementioned methods can be found in [Kalloniatis, 09].

		NFR	***i****	**Tropos**	**KAOS**	**GBRAM**	**RBAC**	**M-N**	**B-S**	**STRAP**	**PriS**
Usage	Requirements Elicitation		✓	✓		✓		✓	✓	✓	✓
	Requirements Specification	✓	✓	✓	✓	✓		✓	✓	✓	✓
	Requirements Validation	✓	✓	✓		✓	✓				
Subject	Overall Business Security and Privacy Requirements	✓			✓	✓	✓	✓	✓	✓	✓
	Security and Privacy Goals of collaborating actors		✓	✓							
	Security and Privacy enabling technologies	✓									✓
	Security and Privacy Policies		✓			✓	✓				
Representation	Graphical notation	✓	✓	✓	✓						✓
	Formal language	✓	✓	✓	✓						✓
Development	Guidance Processes					✓	✓	✓	✓	✓	✓
	Modelling Tools	✓	✓	✓	✓	✓					✓

Table 1: Comparison of Security and Privacy Requirements Engineering Methods

The selection was based on the fact that these methods incorporate basic concepts for the clear representation of security and privacy requirements during the system development and also they study ways for transforming these requirements into specific implementation alternatives. It should be mentioned that none of these methods treat security and privacy as it is described above. Most of them treat security as the main issue and privacy as a single requirement subpart of security. On the other hand, PriS [Kalloniatis, 08] deals with privacy specifically and does not focus on security issues at all.

For strengthening the aforementioned issues it is worth saying that one of the major results of the comparison conducted and presented in Table 1 is that security and privacy issues are not considered with equal significance during the various phases of system development. Another significant drawback is that most of the methods presented stop the analysis before reaching the implementation phase thus failing to successfully guide the designer throughout the whole phases of the system development. Selecting the proper implementation technique has to be the final step of a proper and thorough analysis beginning from the requirements phase and not a single step during the system implementation. However, for the selection to be right security and privacy must be analysed together in order to avoid the aforementioned issues. Another significant drawback that the proposed meta-model overcomes is the way that various methods are dealing with security and privacy issues. Specifically, a number of methods deal with the elicitation of security and privacy requirements only from the organisation's view while others derive the respective requirements from the actors' perspective. However, none of these methods deal with the elicitation of these requirements considering both views. Both ways have positive concepts to offer through system analysis so it is important for a framework to combine both actor and organisational views. Finally, it is observed that every method uses different terminology for expressing similar aspects, for example the privacy goal in PriS [Kalloniatis, 08] is considered as a security constraint in Tropos, as an obstacle in KAOS etc.

Our proposed meta-model combines the concepts that support the analysis of security and privacy concepts considering both organizational and actor view. Based on the issues and the comparison results mentioned above, our proposed framework provides a holistic approach overcoming the drawbacks mentioned by analysing security and privacy from the requirements engineering stage, under a unified framework, based on both actor and organisational views and by ending up suggesting specific implementation technique(s) for the respective security and privacy requirements identified; thus managing to successfully bridge the gap between requirements and implementation phases.

3 Proposed Meta-model

As indicated earlier in the paper, our main aim is to develop an approach to support software engineers to elicit, analyse and reason about security and privacy within a unified framework. An important aspect of such framework is the definition of a modelling language to support it. This section describes our proposed meta-model to support such language, which is based on our previous work in the areas of security and privacy modelling [Kalloniatis, 08], [Kavakli, 07], [Mouratidis, 07a], [Mouratidis, 07b]. In particular, the proposed meta-model combines concepts from security, privacy and requirements engineering. This allows the identification and analysis of security and privacy requirements from the early stages of the software development stages and within social and organizational settings. The rest of this section provides a discussion that highlights the main concepts of the proposed meta-model.

An actor describes an entity that has goals and intentions within the system or within the organisational setting [Yu, 95]. Within the context of our work, an actor has capabilities, which enable her to support the implementation of security and privacy techniques. We also differentiate a special class of an actor, a malicious actor. A malicious actor's intention is to introduce threats to the system, which exploit vulnerabilities. A vulnerability is defined as a weakness or flaw, in terms of security and privacy that exists from a resource, an actor and/or a goal. It is exploited by a threat, as an attack or incident within a specific context. It is worth stating that legitimate actors might unintentionally introduce vulnerabilities to a system due to failure or mistakes. Threats pose potential loss or indicate problems that can put the system in risk. As indicated above, threats are introduced by malicious actors.

A goal represents a condition in the world that an actor would like to achieve [Yu, 95]. Initial elicited goals can be higher level that can be refined to more concrete through AND and/or OR refinement. The refined goals are sub-goals which may contribute to satisfy the higher level goal or may also conflict with the parent goal. Each type of goal is realised by different types of process patterns. For example, a security goal is realised by one or more security process patterns, while a privacy goal is realised by relevant privacy process patterns. Our meta-model differentiates between security and privacy goals, each one of them satisfying a different type of constraint.

Usually, the concept of constraint is used to represent a set of restrictions that do not permit specific actions to be taken, action can be taken in certain way or prevent certain objectives from being achieved and more often are integrated in the specification of existing textual descriptions. However, this approach can often lead to misunderstandings and an unclear definition of a constraint and its role in the development process. Consequently, this results in errors in the very early development stages that propagate to the later stages of the development process causing many problems when discovered; if they are discovered.

Within the context of our work, as indicated above, it is important that both security and privacy constraints are clearly defined as separate concepts to support a clear and well structured elicitation and analysis of security and privacy requirements. We introduce the concept of security constraint, within our work, as a separate concept and we define it as follows: A security condition imposed to an actor that restricts achievement of an actor's goals. A security constraint supports relevant security properties, i. e., confidentiality, integrity, availability and authentication by respecting the security concept and satisfied by relevant security goals. Constraints are outside the control of an actor. Differently than goals, security constraints are not conditions that an actor wishes to introduce but it is forced to introduce based on the system context.

A privacy constraint is defined as a privacy condition imposed to an actor that restricts achievement of an actor's goals. Privacy constraints support relevant privacy properties i.e, anonymity, pseudonymity, and unlinkability, respecting the privacy concept and satisfied by privacy goals. Similar to security constraints, and differently than goals, privacy constraints are not conditions that an actor wishes to introduce but it is forced to introduce based on the system context. In our work, privacy constraints are mainly based on 8 concepts: authentication, authorization, identification, data protection, anonymity, pseudonymity, unlinkability and unobservability. Specifically, authentication is the process of proving the authenticity of an entity. Authorisation is the process of assigning to an entity one or more privileges in order to gain access to one or more assets of a system. Identification has a twofold meaning. Regarding the user that don't belong to the system and try to access one or more services, identification is the process of checking whether personal identifiable information are needed in order for the user to gain access to the system's services. On the other hand, regarding the users belonging to the system, identification is the process of checking whether a specific user is authorized to have access to specific data or not. Data protection is the process of checking the degree of system's conformity and harmonization with the respective directives and laws regarding data handling and manipulation in order to ensure that users' stored data are treated according to the respective legislation. Anonymity is defined as the state of being anonymous or virtually invisible; having the ability to operate online without being tracked [Cannon, 04]. Also it can be defined as the ability of a user to use a resource or service without disclosing his/her identity [Fischer-Hübner, 01]. The outcome of the above definitions is that anonymity serves the great purpose of hiding personal identifiable information when there is no need of revealing them. Pseudonymity is the user's ability to use a resource or service by acting under one or many pseudonyms, thus hiding his/her real identity. However, under certain circumstances the possibility of translating pseudonyms to real identities exists. Pseudonyms are aliases for a user's real identity. Users are allowed to operate under different aliases. Nevertheless revelation of user's real identity occurs when acting unlawfully. Pseudonymity has characteristics similar to anonymity in that user is not identifiable but can be tracked through the aliases he/she uses [Cannon, 04]. Unlinkability expresses the inability to link related information. In particular, unlinkability is successfully achieved when an attacker is unable to link specific information with the user that processes that information. Also unlinkability can be successfully achieved between a sender and a recipient. In that case unlinkability means that though the sender and recipient can both be identified as participating in some communication, they cannot be identified as communicating with each other. The ability to link transactions could give a stalker an idea of your daily habits or an insurance company an idea of how much alcohol your family consumes over a month. Ensuring unlinkability is vital for protecting user's privacy. Finally, unobservability protects users from being observed or tracked while browsing the Internet or accessing a service. Unobservability is similar to unlinkability in the sense that the attacker aims to reveal users identifiable information by observing rather than linking the information he/she retrieves.

A process pattern is defined as a model of how a business in a given domain should be run according to the best practices known. Process patterns convey best practices, and can be used as a guide for business process redesign or for building computer systems to support business processes [Barros, 04]. In our case, we define process pattern considering security and privacy properties that assists in the realization of every security and privacy goal from a number of plans. The process patterns developed are generic enough so as to cover all possible situations of modeling a respective security or privacy goal on a process. For accomplishing the proper degree of generality the application of every security and privacy goal on respective processes using various case studies was conducted so as to ensure that the common steps that the designer needs to follow in order to ensure the application of these patterns on the respective processes were properly addressed. Process patterns are operationalised by relevant plans. A plan defines a specific way of operationalising a process pattern, i.e. the details and conditions under which process pattern is operationalised. Plans are implemented by relevant implementation techniques.

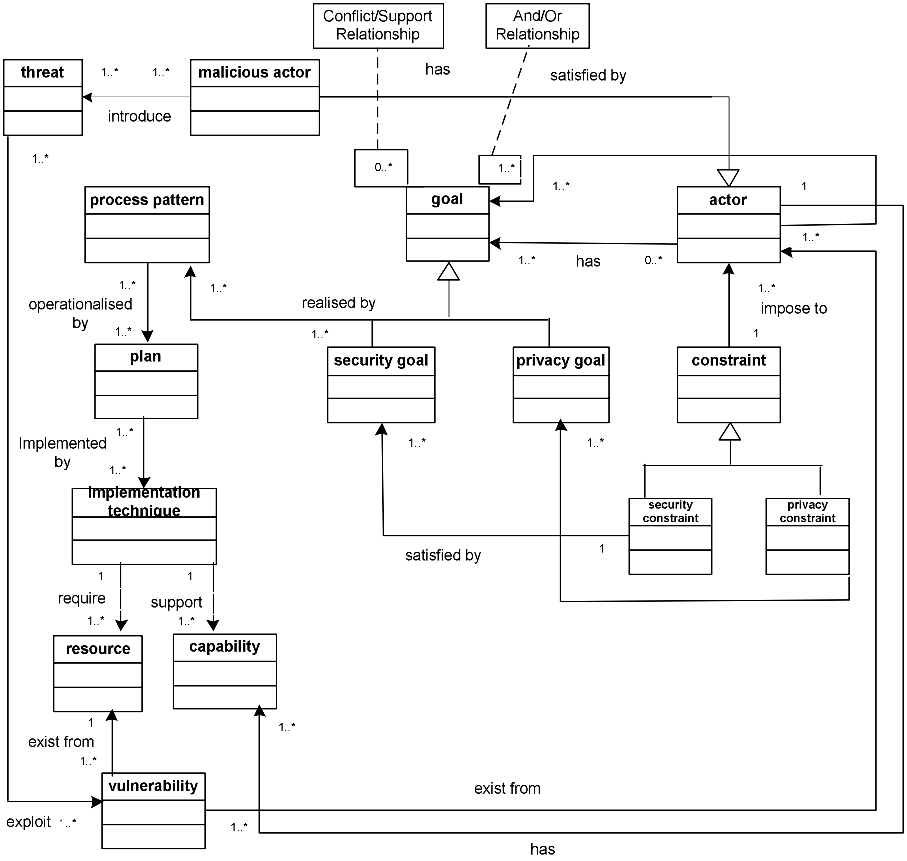

Figure 1: Meta- model for the alignment of security and privacy

An implementation technique is defined as a technical solution that realizes one or more plans. Implementation techniques are software products developed already or customized software tools for realizing plans for the specific organization. Implementation techniques require resources and they are supported by capabilities. This means that in order for an actor to execute an implementation technique a number of required resources may be needed and a number of capabilities should be demonstrated. For example, in case an actor needs to execute the implementation of Onion Routing a number of hardware and software resources are needed (servers, network connections with the intra users as well as with the clients outside the system, demands on process power for the cryptographic calculations etc.). In parallel, this actor may have a number of capabilities that support the realization of the specific implementation technique. For example, the actor may be a process or a software component that has the compatibility to work properly on network environments. In the case of a physical entity the capability of the actor may be its experience in applying the specific implementation technique. Thus, the combination of resources and capabilities leads on the selection of the most appropriate technique for the realization of every plan.

4 The Career Office System Case Study

This section presents the application of the proposed meta- model to a case study based on the University of the Aegean Career Office. A detailed description of the Career Office System can be found in [ICTE-PAN, 05]. We consider different parts of the application which are relevant to the security and privacy concepts. This section starts with an overview of the system and it continues with the identification of relevant security and privacy concepts based on our meta-model.

4.1 The Aegean Career Office System

The main objective of the University of the Aegean Career Office system is to help students to manage the choices and transitions they need to make on ending their studies in order to proceed effectively to the next step of their life.

The career office system is described by three main principles that form the three primary organisational goals namely: a) Provide Career Information, b) Offer Guidance through Events and c) Maintain a lifelong communication with the graduates. In our work, Organisational goals are derived from the important objectives of an organisation that need to be accomplished by the system under development. Usually an organisation’s stakeholders, who have great business interests, assist on forming organisational goals. Other sources of elicitation are strengths and weaknesses, opportunities or threats that analysts take under consideration when defining the set of organisational goals that need to be accomplished. Generally, organisational goals express the intentional objectives that control and govern an organisation’s operation. Regarding the organisational goals of our case study, the first goal implies the career office should maintain a career information system, which will be continuously updated from various sources (press, job and company web-sites etc), and will provide open access to the academic community. The second goal implies that the career office will provide educational, vocational and careers guidance to the students through particular events and organize summer jobs for the undergraduate students. Finally, the third goal implies the career office will maintain a lifelong relationship with graduate students concerning relevance to employment.

4.2 Application of the proposed conceptual model

The initial step of the analysis, based on the proposed meta-model model, is the identification of the main actors of the system. Specifically, there are three main actors in the system:

- Graduate
- Employee
- Career office system

At this stage, goals are constructed and processes are realized based on the organizational context by following the Enterprise Knowledge Development framework [Loucopoulos, 99], [Loucopoulos, 00]. The produced goal model is presented in Figure 2. As stated previously, three organizational goals are identified which are refined into sub-goals and finally satisfied by processes. The doted boxes are the relevant processes satisfying each sub-goal. Note that to demonstrate the case study we continue with goal G3 along with the integrity and anonymity constraints. For instance the goal G3 is refined into the following way:

Main goal:

- Maintain lifelong communication with the graduate (G3)

Sub-goal:

- Publish a Newsletter for the graduates of the University (G 3.1)
- Maintain Contact and have co-operation with the graduates associations (G 3.2)
- Make follow up research concerning the professional progress of the graduates by sending them questionnaires (G 3.3)
- Send regularly to graduates electronic information about public and private sector openings (G 3.4)

Relevant process:

- Conduct graduates survey (P4)

Relevant sub- process:

- Collect Responses (P4.3)

In particular, for conducting the graduates' survey, the career office sends questionnaires to all university graduates. Specifically, the career office is creating a database with the contact details of all the graduates of the University of the Aegean. It receives the relevant data from the secretariats of each Department and compares them with the data it has collected from the previous graduate's survey. Then questionnaires are posted to the career office portal. Emails are sent to graduates with a link to the corresponding page in the career office's portal. For graduates without an email, a letter is posted with the questionnaire and a return envelope with a pre-paid postage stamp. Responses are then collected either through the career office's portal or by email. Based on the organizations context graduates must be ensured that nobody especially malicious third parties will be able to reveal the name or other elements that may lead to the identification of the graduate that submits the answered questionnaire.

This is the major threat that can occur which will lead to a privacy violation. The data must be summarized based on the graduate response on the questionnaire so that authority can obtain the employability status of the university based on offered program as well as the graduate expectations for the employability. Therefore, integrity of the data summarization is necessary which can be violated by internal attack in particular from the employee of the career office. Vulnerability from data or actor to pose any attack like spoofing, unauthorized modification needed to be prevented.

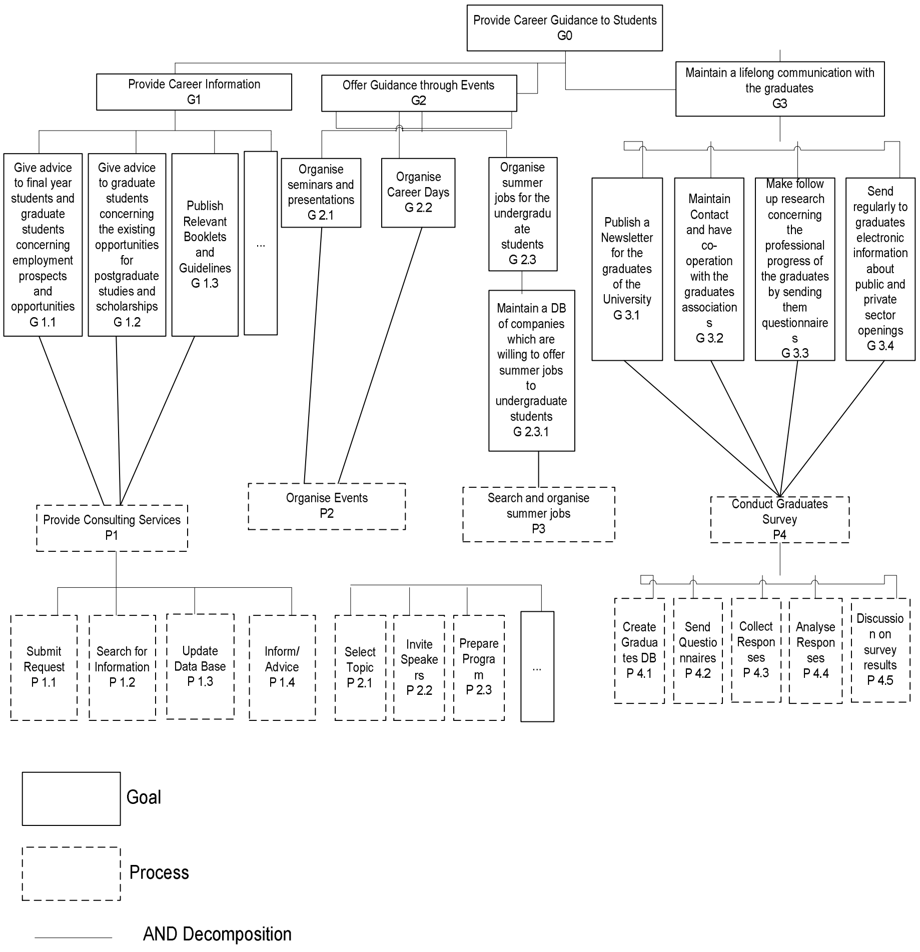
Provide Career Guidance to Students G0
Provide Career Information G1
Offer Guidance through Events G2
Maintain a lifelong communication with the graduates G3
Give advice to final year students and graduate students concerning employment prospects and opportunities G 1.1
Give advice to graduate students concerning the existing opportunities for postgraduate studies and scholarships G 1.2
Publish Relevant Booklets and Guidelines G 1.3
...
Organise seminars and presentations G 2.1
Organise Career Days G 2.2
Organise summer jobs for the undergraduate students G 2.3
Maintain a DB of companies which are willing to offer summer jobs to undergraduate students G 2.3.1
Publish a Newsletter for the graduates of the University G 3.1
Maintain Contact and have co-operation with the graduates associations G 3.2
Make follow up research concerning the professional progress of the graduates by sending them questionnaires G 3.3
Send regularly to graduates electronic information about public and private sector openings G 3.4
Provide Consulting Services P1
Organise Events P2
Search and organise summer jobs P3
Conduct Graduates Survey P4
Submit Request P 1.1
Search for Information P 1.2
Update Data Base P 1.3
Inform/ Advice P 1.4
Select Topic P 2.1
Invite Speakers P 2.2
Prepare Program P 2.3
...
Create Graduates DB P 4.1
Send Questionnaires P 4.2
Collect Responses P 4.3
Analyse Responses P 4.4
Discussion on survey results P 4.5
Goal
Process
AND Decomposition

Figure 2: Goal Model of the University of the Aegean Career Office System

The next step involves the consideration of basic security and privacy concerns, which are relevant to the case study context, based on the organizational goals defined earlier. The above analysis assists in identifying the main privacy and security constraints that need to be realized for our case study, i.e. the main privacy constraint that needs to be realized is anonymity and the main security constraint that needs to be realized is integrity. For reasons of simplicity in this paper we present the analysis of just these main constraints. Specifically, when graduates send information through the career office portal it must be ensured that others won't be able to reveal their personal identifiable information (anonymity) and data must be retain without any unauthorized modification (integrity). However, these constraints are rather high level and require refinement. Based on our meta-model the refinement is accomplished by identifying for every constraint the respective security or privacy goal so as to determine more specifically what the system needs to achieve. Then the respective processes are identified along with the process patterns which assist in the selection of the proper implementation techniques through the realization of a plan for every pattern.

To achieve the former, it is important to identify what organizational goal and sub-goals are constrained, by those constraints, in order to realize anonymity and integrity. Both constraints have impact on Goal G3: Maintain a lifelong communication with the graduates and its sub-goal G3.3: Make follow-up research concerning the employment and the professional progress of the graduates of the University by sending questionnaires to the graduates. It is clear that in order to successfully realise the anonymity constraint applied on the aforementioned organization goal and sub-goal a new privacy goal needs to be introduced that will carry the task of satisfying that specific privacy constraint. Similar, integrity needs to be ensured for compiling the collected response. In particular, the summary of the response must reflect the view provided by the graduates. Thus a security goal is also introduced in order to satisfy the integrity constraint of goal G3.3. The actor which will try to accomplish this goal is obviously the career office system and career office employee. The security and privacy goals are:

- Collect Graduates' responses ensuring their anonymity (Privacy Goal)
- Ensure integrity of summarized data which are based on the collected response (Security Goal)

To realise the privacy goal, an anonymity process pattern is presented in Figure 4 based on the process patterns shown in Figure 3. Therefore Figure 4 represents the patterns by following the case study context. Figure 5 shows the pattern for summarizing the response by following the integrity constraint. By applying the respective process pattern on the relevant security/privacy goals it is easier for the designer to identify the appropriate plans that will assist in the successful implementation of the respective goals. Also process patterns assist on bridging the gap between generic security/privacy goals and specific/technical plans.

Also the identification of possible malicious actors needs to be realised before the analysis proceeds to the identification of the respective process patterns. Malicious actors may introduce threats that will violate the integrity of the results or they may take advantage of specific system vulnerabilities which may lead to the identification of students' identity and linking data to the respective questionnaires which they've sent. Internal actors, and in particular graduate and employee, can be malicious actors for the first threat, while eavesdroppers and external actors, who might tamper the communication lines and server ports, can be the main malicious actors for the second threat.

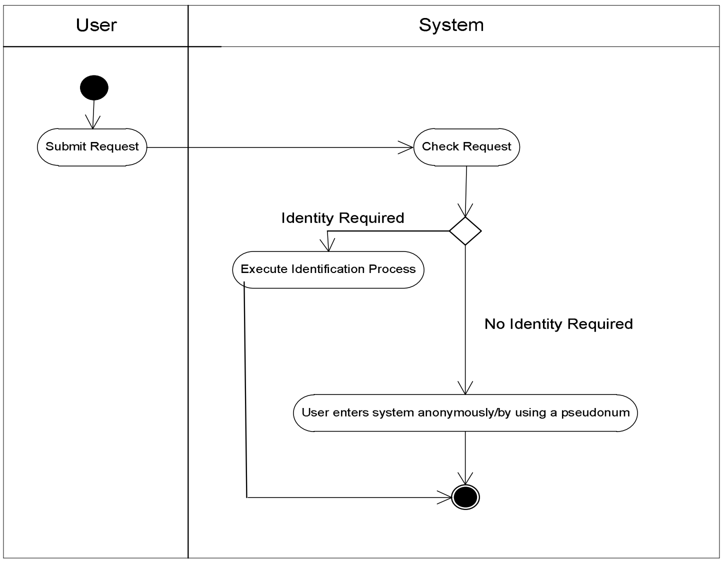
User
System
Submit Request
Check Request
Identity Required
Execute Identification Process
No Identity Required
User enters system anonymously/by using a pseudonum

Figure 3: Anonymity-Pseudonymity Process Pattern

The next step involves the identification of plans, which aim to operationalise the respective process patterns, as well as to protect against potential threats being realised. Based on our analysis, the following plans were proposed for the realisation of the integrity goal:

- Check integrity
- Compile log from the response
- Provide validation for the questionnaire response

And the following for the privacy goal:

- Check Necessity of Identification Mechanism
- Provide anonymous communication between the sender and the system

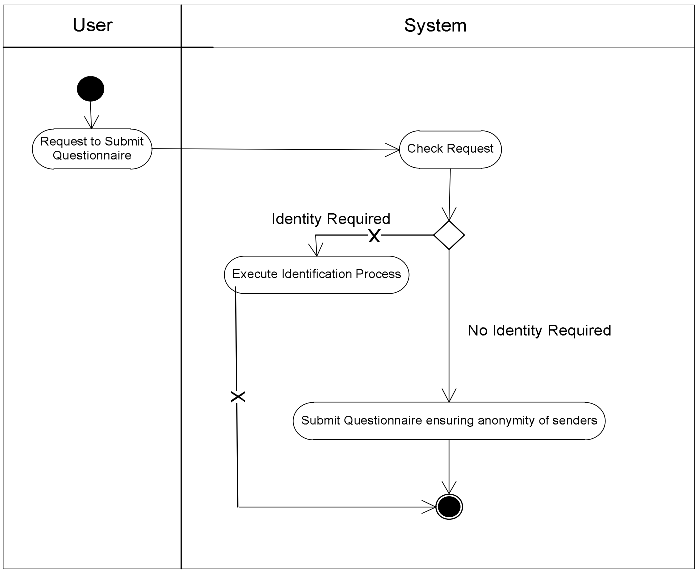
User
System
Request to Submit Questionnaire
Check Request
Identity Required
Execute Identification Process
No Identity Required
Submit Questionnaire ensuring anonymity of senders

Figure 4: Application of Anonymity-Pseudonymity Process Pattern

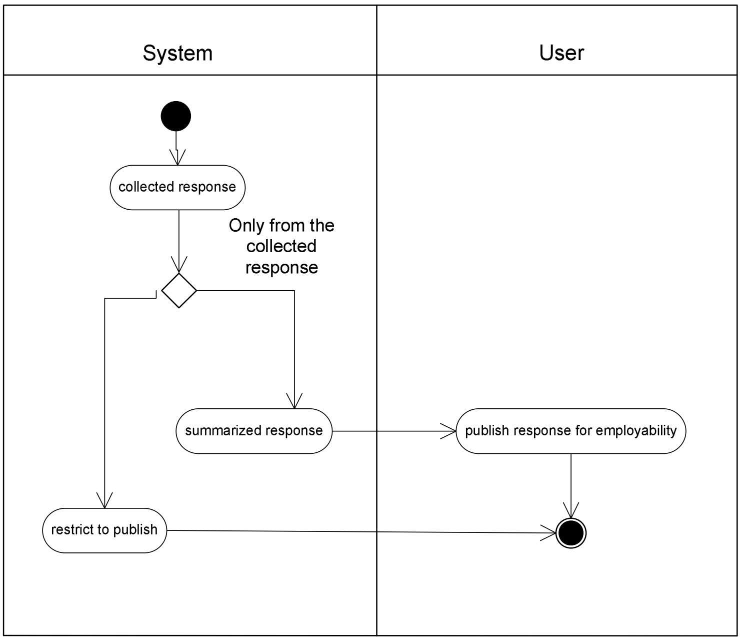
System
User
collected response
Only from the collected response
summarized response
publish response for employability
restrict to publish

Figure 5: Process Pattern for summarized response

For realising the plans presented above a number of implementation techniques are identified and suggested. Implementation techniques along with resources and capabilities are necessary for implementing the plans. Our implementation techniques include tools and are considered as critical classes of the system which collect the graduate response and summarize the data. Therefore for our case study the following techniques are applicable:

- Administrative and anonymizer tools
- Class and its functionalities to compile and summarize the collected response

Meta-element	**Security**	**Privacy**
Constraint	Integrity	Anonymity
Goal	Ensure integrity of summarized data which are based on the collected response	Collect Graduates' responses ensuring their anonymity
Actor	i) Career Office System ii) Career Office Employee	Career Office System
Malicious Actor	i) Graduate ii) Employee	External actors-eavesdroppers
Threat	Spoofing or unauthorized modification of the data summarization	Reveal the name or other elements that may lead to the identification of the graduate that submits the answered questionnaire.
Process Pattern	Integrity Process Pattern	Anonymity Process Pattern
Plan	i) Check integrity ii) Compile log from the response iii) Provide validation for the questionnaire response	i) Check Necessity of Identification Mechanism ii) Provide anonymous communication between the sender and the system
Implementation Technique	Class and its functionalities to compile and summarize the collected response	Administrative and anonymizer tools
Resources	i) Log file ii) Graduate response and summarized data	i) Onion routing/tor for the anonymizer ii) Identity management for the administrative tool

Table 2: Mapping of case study analysis to meta-model concepts

Finally, our analysis considers resources, which are required for implementing plans. In our specific case the resources identified are:

- Identity management for the administrative tool
- Onion routing/tor for the anonymizer

- Log file
- Graduate response and summarized data

Table 2 illustrates a mapping of the security and privacy concepts of the case study to the meta-model concepts.

In this section, we applied the proposed meta-model on the University of the Aegean Career Office System to illustrate the approach. The model starts with identifying the main actors within the organizational context. Based on the actors and organization goals main constraints are identified which need to be ensured for the proper operation of the system. These security and privacy constraints guide which operations are required and satisfy the security and privacy goals. The goals are then realised by process patterns and operationalised by plan. At the same time, the possible vulnerability, threat and malicious actor are also analysed. This allows selecting the appropriate implementation technique to support the plan so that process can be properly operated. Therefore the model supports to identify, reason and analysis security and privacy constraints until the implementation techniques that satisfy these constraints from both organizational and actor view. It is an unified approach to analyse security and privacy and align the artefacts to meet the overall system goals.

5 Related Work

A number of researchers have already contributed in the area of identifying and analysing security and privacy properties for the development of software systems in particular in the context of requirements specification.

Mouratidis et al. [Mouratidis, 07a] present Secure Tropos as a security goal-driven approach for integrating security related concepts into the Tropos methodology. The approach considers security constraints such as integrity throughout the development stage, from the early requirements analysis to the implementation. These constraints can be effective in eliciting and analysing the security requirements. The approach is further extended Secure Tropos with the notion of security attack scenarios [Mouratidis, 07b], where possible attackers, their attacks and system resources that can be attacked are modelled.

Houmb et al. introduce SecReq approach to elicit, analyse the trace the security requirements from requirements engineering phase to design using Common Criteria, Heuristic and UMLsec [Jürjens, 05], [Houmb, 10]. Sindre et al. [Sindre, 05] propose a misuse case driven approach to elicit security requirements at an early stage. Mead et al. [Mead, 06] propose the SQUARE (Security Quality Requirements) method for eliciting, analysing, and documenting security requirements. Haley et al. [Haley, 06] provide an approach for security requirements elicitation, specification and analysis. Furthermore, Mellado et al. [Mellado, 07] present SREP (Common Criteria based security requirements engineering process), where several Common Criteria constructs have been employed (e.g. security functional components, protection profile, and security assurance components) for eliciting security requirements. Both SREP and SQUARE are asset-based and risk-driven methods for eliciting, categorising, and prioritising security requirements. However, SREP differs from

SQUARE as it integrates knowledge and experience from the Common Criteria and Information Security Standards, such as ISO/ IEC 27001, while eliciting security requirements. SecReq also uses Common Criteria part two to elicit security requirements from security objective and functional requirements. SecReq traces the identified requirements to the system design using UMLsec stereotypes.

Kalloniatis et al. [Kalloniatis, 08], [Kalloniatis, 09] introduces the PriS method which incorporates privacy requirements early in the system development process. PriS considers privacy requirements as organizational goals that need to be satisfied and adopts the use of privacy process patterns as a way to: (a) describe the effect of privacy requirements on business processes; and (b) facilitate the identification of the system architecture that best supports the privacy-related business processes. Siena et al. in [Siena, 09] identified software requirements considering relevant laws and legislation. Breaux et al. [Breaux, 08] consider activity, purpose and rules to extract rights, obligations and constraints from legal texts. Rights and obligations are the actions that stakeholder are permitted and required to perform. In this work, extracted rights and obligations are stated into restricted natural language statements to depict discrete activities, in an application context, based on a semantic parameterization process. Bellotti and Sellen [Bellotti, 93] developed a framework for privacy-aware design in the field of ubiquitous computing. This framework proposes a procedure designers may follow through a set of questions in order to evaluate a system. The evaluation is accomplished by identifying a set of new requirements, which must be implemented by the developers, purpose, and rule sets to extract rights, obligations, and constraints from legal texts. Massey et al. [Massey, 09] propose four methodological activities to evaluate existing security and privacy requirements for legal compliance. The approach in particular prioritises the requirements and establishes traceability links from requirements to legal texts. Islam et al. [Islam, 11] analyse the legal text by using legal taxonomy so that legal requirements can be extracted and map with the security requirements. The approach aligns legal requirements with security requirements by using Secure Tropos and traces it into design using UMLsec. Islam et al [Islam, 10a] presents a framework to elicit and analyse security and privacy requirements from laws and regulation. Islam et al in [Islam, 10b] introduced Goal-driven Software Development Risk Management model (GSRM) to assess and manage the risks from the early stage of the development. He et al. in [He, 03] proposed goal based framework for modelling privacy requirements. Here context and constraints are used to model the privacy requirements through goal based RE techniques. Authorization rules such as access control rules are followed to formulate the natural language that contains privacy policies and requirements. User can only access to an object if specific role that contain permission (i.e. operations to the object) to access the object is assigned to the user.

We follow some of these contributions as base line foundation for our work such as SecureTropos and PriS. However, our model demonstrates a number of novel contributions. It enables the analysis of security and privacy issues and inter-relates them within the organizational and actor settings. Moreover, we focus on bridging the gaps from the requirements to the implementation solutions by identifying and analysing the requirements and mapping them with the process so that relevant implementation solutions are identified.

6 Future Work

Security and privacy practices are important factors for software that manages sensitive information and for the stakeholder when selecting software or service providers to serve their business needs. This paper contributes to the realisation of software systems that support security and privacy. Our approach initially supports the consideration and analysis of security and privacy constraints and their realisation using process patterns, plans and implementation techniques. Therefore the proposed model concerns not only with the identification and analysis of the relevant (security and privacy) requirements but also focuses on the implementation techniques to support these requirements. A case study has been used in the paper to demonstrate the applicability of our work.

Our main aim is to develop a framework that will support every step of the development process focusing on security and privacy aspects of a software system. The proposed conceptual model and the work presented in this paper constitute a first step in that direction. Our next step involves the definition of specific development processes to better support the presented conceptual model. Moreover, we also work on the development of automated tools to support our work.

References

[Antón, 00] A. Antón, and J. Earp, Strategies for developing policies and requirements for secure electronic commerce systems. 1st Workshop on security and privacy in e-commerce. ACM,2000.

[Barros, 04] O. Barros, Business Process Patterns and Frameworks: Reusing Knowledge in Process Innovation, Technical Report 56, Universidad de Chile , 2004. [Cocoon, 02] Cocoon XML publishing framework, 2002, http://xml.apache.org/cocoon/

[Bellotti, 93] V. Bellotti, A. Sellen, Design for Privacy in Ubiquitous Computing Environments, In: Michelis, G., Simone, C., Schmidt, Kjeld (ed.), Proceedings of the Third European Conference on Computer Supported Cooperative Work - ECSCW 93 pp. 93-108,1993.

[Breaux, 08] T. D. Breaux and A. I. Antón, Analyzing Regulator Rules for privacy and Security Requirements, IEEE transactions on software engineering, Vol. 34, No. 1, January-February 2008.

[Cannon, 04] J. Cannon, Privacy, What Developers and IT Professionals Should Know. Addison-Wesley, 2004.

[Chung, 93] L. Chung, Dealing with security requirements during the development of information systems. The 5th international conference of advanced information systems engineering, CAiSE'93, Paris, France, Springer Verlag LNCS 685, pp: 234-251,1993.

[Fischer-Hübner, 01] S. Fischer-Hübner, IT-Security and Privacy, Design and Use of Privacy Enhancing Security Mechanisms. Lecture Notes in Computer Science, Vol. 1958. Springer-Verlag, Berlin , 2001.

[Haley, 06] C.B. Haley, R. Laney, J.D. Moffett and B. Nuseibeh, Arguing Satisfaction of Security Requirements, in Integrating Security and Software Engineering: Advances and Future Visions, pp. 16- 43, Idea Publishing Group, 2006.

[He, 03] Q. He, A.I. Antón, A framework for modelling privacy requirements in role engineering. In: Proceedings of the 9th International Workshop on Requirements Engineering: Foundation for Software Quality (REFSQ'03), Austria, 2003.

[Houmb, 10] S. H. Houmb, S. Islam, E. Knauss, J. Jürjens, and K. Schneider. Eliciting Security Requirements and Tracing them to Design: An Integration of Common Criteria, Heuristics, and UMLsec. Requirements Engineering Journal, 15(1):63–93, March 2010.

[ICTE-PAN, 05] ICTE-PAN: Methodologies and Tools for Building Intelligent Collaboration and Transaction Environments in Public Administration Networks, Project Deliverable D 3.1b, 2005, University of the Aegean, Greece.

[Islam, 10a] S. Islam, H. Mouratidis and S. Wagner, Towards a Framework to Elicit and Manage Security and Privacy Requirements from Laws and Regulations, In Proc. of 16th International Working Conference on Requirements Engineering: Foundation for Software Quality (REFSQ '10), Springer-Verlag, 2010. Essen, Germany.

[Islam, 10b] S. Islam and S. H. Houmb, Integrating Risk Management Activities into Requirements Engineering, In Proc. of the 4th IEEE Research International Conference on Research Challenges in IS (RCIS2010), Nice, France.

[Islam, 11] S. Islam, H. Mouratidis and J. Jürjens, A Framework to Support Alignment of Secure Software Engineering with Legal Regulations, Journal of Software and Systems Modeling (SoSyM), Theme Section on Non-Functional System Properties in Domain-Specific Modeling Languages (NFPinDSML), 2011, Springer-Verlag.

[Jensen, 05] C. Jensen, J. Tullio, C. Potts and E. Mynatt, STRAP: A Structured Analysis Framework for Privacy. GVU Technical Report, Georgia Institute of Technology, GIT-GVU-05-02,2005.

[Jürjens, 05] J. Jürjens. Secure Systems Development with UML. Springer, 2005.

[Kalloniatis, 08] C. Kalloniatis, E. Kavakli, and S. Gritzalis, Addressing privacy requirements in system design: The PriS method, Requirements Engineering, 13(3): 241-255,2008.

[Kalloniatis, 09] C. Kalloniatis, E. Kavakli, S. Gritzalis, Methods for Designing Privacy Aware Information Systems: A review, Proceedings of the PCI 2009 13th Pan-Hellenic Conference on Informatics (with international participation), N. Alexandris, V. Chryssikopoulos, C. Douligeris, N. Kanellopoulos (Eds.), September 2009, Corfu: Greece, IEEE CPS Conference Publishing Services.

[Kavakli, 07] E. Kavakli, S. Gritzalis, and C. Kalloniatis, C. (2007), Protecting Privacy in System Design: The Electronic Voting Case, Transforming Government: People, Process and Policy, 1(4): 307-332.

[Koorn, 04] R. Koorn, H. van Gils, J. ter Hart, P. Overbeek, and R. Tellegen, Privacy Enhancing Technologies, White paper for Decision Makers. Ministry of the Interior and Kingdom Relations, the Netherlands, December 2004.

[Letier, 00] E. Letier and A. van Lamsweerde, Deriving operational software specifications from system goals. 10th ACM SIGSOFT International Symposium on the Foundations of Software Engineering pp: 119-128,2000.

[Loucopoulos, 00] P. Loucopoulos, From Information Modelling to Enterprise Modelling. In: IS Engineering: State of the Art and Research Themes. Springer, 2000, 67-78.

[Loucopoulos, 99] P. Loucopoulos, V. Kavakli, Enterprise Knowledge Management and Conceptual Modelling. LNCS Vol. 1565. Springer,123-143,1999.

[Massey, 09] A. K. Massey, P. N. Otto, L. J. Hayward, and A. I. Antón, Evaluating existing security and privacy requirements for legal compliance, Requirements Engineering Journal, Special issues security requirements engineering, 2009.

[Mead, 06] N.R. Mead, Identifying Security Requirements Using the Security Quality Requirements Engineering (SQUARE) Method, Integrating Security and Software Engineering, pp. 44-69, Idea Publishing Group, 2006.

[Mellado, 07] D. Mellado, E. Medina, and M. Piattini, A common criterion based security requirements engineering process for the development of secure information system. Computer standards & interfaces, 29:244– 253, June 2007.

[Moffett, 95] D. Moffett and B. Nuseibeh, A framework for security requirements engineering. Department of computer science, University of York, YCS 368, 2003.

[Mouratidis, 06] H. Mouratidis and P. Giorgini, Integrating Security and Software Engineering: Advances and Future Visions, Idea Group Publishing, 2006.

[Mouratidis, 07a] H. Mouratidis and P. Giorgini, Secure Tropos: A Security-Oriented Extension Of The Tropos Methodology, International Journal of Software Engineering and Knowledge Engineering, 2007 © World Scientific Publishing Company.

[Mouratidis, 07b] H. Mouratidis and P. Giorgini, Security Attack Testing (SAT) - testing the security of information systems at design time. Inf. Syst. 32(8): 1166-1183, 2007.

[Siena, 09] A. Siena, J. Mylopoulos, A. Perini, and A. Susi. Designing Law-Compliant Software Requirement, LNCS, Volume 5829/2009, 28th International Conference on Conceptual Modeling (ER2009), Gramado, Brazil.

[Sindre, 05] G. Sindre and A. L. Opdahl, Eliciting Security Requirements with Misuse Cases, Requirements Engineering, 10(1):34-44, January 2005.

[Yu, 93] E. Yu. Modeling organisations for information systems requirements engineering. 1st IEEE International Symposium on Requirements Engineering pp: 34-41, 1993.

[Yu, 95] E. Yu, Modelling Strategic Relationships for Process Reengineering, Ph.D. thesis, Department of Computer Science, University of Toronto, Canada, 1995.