Towards a Framework to Elicit and Manage Security and Privacy Requirements from Laws and Regulations

Shareeful Islam[1], Haralambos Mouratidis[2], Stefan Wagner[3]
[1,3]Institut für Informatik, Technische Universität München, Germany
[2]School of Computing, IT and Engineering, University of East London, Great Britain
[1,3]{islam,wagnerst}@in.tum.de, [2] haris@uel.ac.uk

Abstract. [**Context and motivation**] The increasing demand of software systems to process and manage sensitive information has led to the need that software systems should comply with relevant laws and regulations, which enforce the privacy and other aspects of the stored information. [**Question/problem**] However, the task is challenging because concepts and terminology used for requirements engineering are mostly different to those used in the legal domain and there is a lack of appropriate modelling languages and techniques to support such activities. [**Principal ideas/results**] The legislation need to be analysed and align with the system requirements. [**Contribution**] This paper motivates the need to introduce a framework to assist the elicitation and management of security and privacy requirements from relevant legislation and it briefly presents the foundations of such a framework along with an example.

Keywords: Security requirements, privacy requirements, Secure Tropos, modelling, and evolving legislation.

1. Introduction

Software systems are now widely used for applications including financial services, industrial management, and medical information management. Therefore, it is now necessary that software for critical applications must comply with the relevant legislation. Sensitive system information must not be open to unauthorised access, processing, and disclosure by legitimate users and/or external attackers. This situation makes security to one of the key components involved in ensuring privacy [1]. Information security and data privacy laws are in general complex and ambiguous by nature and in particular relatively new and evolving [2, 10].

Such laws often undergo evolution to support the demands of the volatile world. Several factors such as the introduction of new restrictions, regulation mandates to increase security, privacy and quality of service, technology evolution, and new threats and harms are commonly responsible for the amendment of legislation. An amended legislation enforces an organization to review their internal policies and to adopt the changes in their software systems. Especially legally relevant requirements (security and privacy in our case) should be adapted to avoid corresponding risks. Therefore, research should be devoted to the development of techniques that systematically extract and manage requirements from laws and regulations in order to support requirements compliance to such laws and regulations. We believe evolution

at requirements level is critical in order to meet the needs of its stakeholders and the constraints such as legal requirements so that change can be traced further through the life cycle. Due to the above situation, the elicitation of legally compliant requirements is a challenging task.

This paper, as an extension of our previous work [9], discusses the need to introduce a framework to allow the elicitation and management of security and privacy requirements from relevant laws and regulations and it briefly presents the foundations of a novel framework that assists in eliciting security and privacy requirements from relevant legislation and it supports the adoption of changes in the system's requirements to support the evolution of the laws and regulations. Our contribution addresses the current research problem of handling evolution of laws, regulation and their alignment to the requirements.

2. Overview of the Framework

The framework is based on the Secure Tropos modelling language [4, 5] and goal-driven security risk management (GSRM) [8]. It includes four main activities and each consists of several steps that support the purpose of the activity and produces artefacts. One of the main input elements required for performing the activities are relevant legal texts. Therefore business specifications including business goals, process, and an initial set of user requirements are required to identify the relevant legal text. Figure 1 shows an overview of the framework with the input documents, activities, and steps in the activity, artefacts produced from the activities, and the associated links.

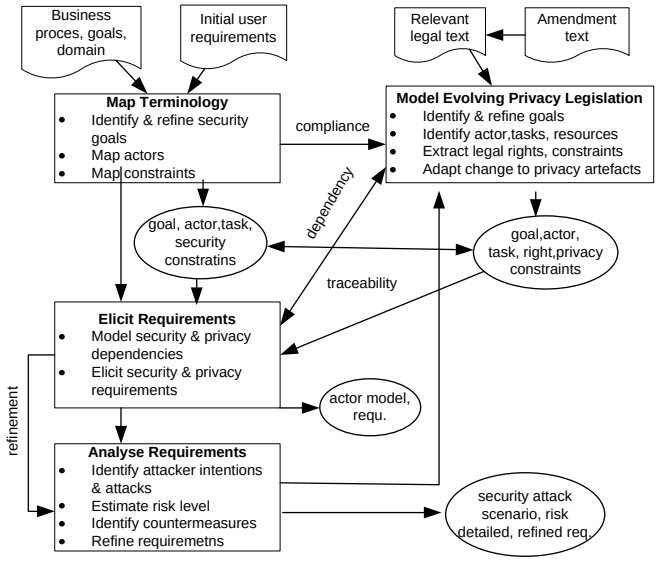

Fig. 1. Overview of the framework

Activity 1: Model Evolving Regulation. The first step in that activity is to identify and refine the goals from the privacy legislation by analysing why the regulation and

specific sections of the regulation were introduced to support the specific context. We follow a basic legal taxonomy proposed by Hohfeld [11] to identify the terms of privacy legislation. The taxonomy is based on legal rights and classifies in several elementary concepts including privilege, claim, power, immunity, duty, no-right, liability, and disability. The next step involves the identification of the relevant actors, their performed tasks, and the required resources in the system environment to support the goals. Legal rights are concerned with the actions that the actors are allowed or permitted to perform [10, 11]. The rights should focus on certain *consent*, *enforcement*, *notice*, *awareness*, and *participation* relating to the privacy taxonomy [1]. We use activity and purpose patterns [10] along with a sub-set of the Secure Tropos language to support these steps [4]. The final step involves the adoption of privacy artefacts with the legislation evolution. We consider the privacy artefacts identified previously to support the analysis of the requirements' change and we structure our analysis into three possible ways, with which legal text evolves [7]: addition of a new clause, modification of an existing clause, deletion of a clause.

Activity 2: Map Terminology. During this activity legal terms are mapped to the terms used for security and privacy requirements. In particular, the legal artefacts identified from the previous activity are systematically mapped to the security artefacts. An initial step is to identify and refine the security goals. Security goals are identified by analysing the business and initial user requirements of the system environment, and by following the privacy taxonomy [1]. The main focus is to ensure critical security properties such as confidentiality, integrity, availability, authenticity, and non-repudiation as well as the privacy goals from the previous activity within the overall system environment. Once the goals are identified, the next step is to map the actors from the legal concepts to the security concepts by following both security and privacy goals. Finally we need to map the privacy and security constraints for the goal satisfaction by following goals, actors, and task.

Activity 3: Elicit Requirements. During the first step of this activity, we model the secure and privacy dependencies through the Secure Tropos actor model [4], by following the identified actors, goals, tasks, and constraints. This allows us to establish the compliance link from the legal concepts to security concepts. Finally security and legal requirements are identified by elaborating both security and privacy constraints and traceability from legal concepts to security is attained through the identified artefact; in particular by following the relevant goals, tasks, and actors.

Activity 4: Analyse Requirements. This final activity refines the initial requirements by following risk and evolution techniques. Security threats and privacy harms that obstruct the relevant goals and influence the relevant non-compliance issues are identified and analysed. To support the analysis, we combine goal-driven risk management [8] with Security Attack Scenarios (SAS) [5]. The activity starts by identifying the attacker's intentions and attacks. This allows us to identify the potential resources of the system that might be attacked. In our framework, we model the goals of an attacker, attacks and possible resources of the system that might be attacked with an extended set of *attack links* [5]. The next step of the activity is to estimate the risk level based on the analysis techniques of GSRM so that risks are categorised as *high*, *medium*, and *low* by focusing on the risk likelihood and impact. Once the risks are estimated then it is important to identify the countermeasures to prevent the potential attacks and non-compliances issues. Finally the initial

requirements are refined (if needed) to accommodate provisions for the countermeasure of attacks that cannot be prevented with the existing set of requirements.

3. Example

The presented example briefly illustrates the applicability of our framework to a specific application context, where a German bank that offers its customers use of a smart card (EC card) for payments. We have chosen relevant privacy regulations by considering the EU directive 95/46/EC [6] and German Federal Data Protection Act (FDPA) [3] that are related for the context. In the text below, normative phrases (such as "must", "shall") and conditional phrases (such as "and", "or") are in bold; a subject for an action is underlined; an action is italicized; an object is in bold and underlined; a measurement parameter is in bold, italicized, and underlined.

Directive 95/46/EC, Article 17 (partial), Security of processing (partial)

1. Member States shall provide that the controller **must** implement ***appropriate technical and organizational measures*** to *protect* **personal data against** accidental **or** unlawful destruction **or** accidental loss, alteration, unauthorized disclosure **or** access, in particular where the processing involves the *transmission* of ***data*** over a network, **and** against all other unlawful forms of processing. Having regard to the state of the art and the ***cost*** of their implementation, such ***measures*** **shall** ensure a ***level of security appropriate to the risks*** represented by the processing and the nature of the **data** to be protected.

German Federal Data Protection Act, Annex (partial)

1. To prevent unauthorised persons from gaining *access* to data processing systems with which ***personal data*** are *processed* **or** *used* (access control).

Activity 1: Model Evolving Regulation. The goal of 95/46/EC is to ensure *personal data protection*, which is refined with *security in processing* and supported by *appropriate technical and organisational measures* in article 17. The FDPA supports the goal of 95/46/EC by including high level requirements such as *access control* in its annex. The *customer* and *application providers* are the two main actors. *Customer data* is the main resource, which contains personally identifiable information such as the customer name and sensitive information such as card and account details. The resource is shared for common tasks such as *collect customer data*, and *update account balance*. Among the identified legal rights is that the providers have the liability to take appropriate measure to ensure privacy protection and to protect from any accidental and unlawful activities. To simplify the illustration of our framework, at this stage, we have not considered any evolution of legal texts but we consider it during the analysis activity below.

Activity 2: Map Terminology. The security goal for the application context is already considered by the legal goals. Therefore, we directly refine the goals to support the security properties. For example, *access control* is refined to *identification and adequate authorisation*. Goals such as *data integrity* and *secure communication* as well as tasks like *providing customised reports about balance* are necessary for this context. To map actors, for simplicity, we consider high level actors such as bank and card issuer and assume their roles support the security constraints. The security constraints supported by the actors are: *only legitimate customer*, *keep communication secure*, *transfer minimum data*, and *preserve anonymity*. Finally, security and privacy constraints are mapped to align with the goals, such as providers' liability to consider

any technical measure as privacy constraints and only legitimate customer, keep communication secure as security constraints support goals like access control, and secure communication.

Activity 3: Elicit Requirements. Once the security and privacy constraints are analysed, this activity initially models their dependencies and then elicit relevant requirements such as; i) The customer shall be identified and authenticated before allowed to perform any transaction through the card; ii) The bank shall only provide the minimum of required data to the retailer that supports the business purpose.

Activity 4: Analyse Requirements. Finally, the elicited requirements are analysed based on the security threat, privacy harm, and legislation evolution. We consider *data retainment* from directive 2006/24/EC [6] as evolution by adding new constraints from the legislation to the application context.

Article 6 partial (Periods of retention)

Member States shall ensure that the **categories of data** specified in Article 5 are *retained* for periods of not less than six months and not more than two years from the date of the communication.

The amendment of the legal text introduces the bank's liability to retain the customer data for a certain period to time. At this stage, we need to identify the attacker intentions and attacks for the non-compliance issues in the environment. Among the several attackers' goals, we consider here *obtain sensitive data*, by external attackers through unauthorised access to the system or eavesdropping, and by internal attackers through misuse. Furthermore, amendment of legislation also supports the attacker's goal, as the longer data is retained, the higher the likelihood of accidental disclosure, data theft, and other illegal activities. Commonly the impacts of the factors are high once the attacker successfully performs any attack. Therefore, for simplicity we consider the risk level as high for both high and medium likelihoods of the risk factors. Finally, requirements are refined such as, the data shall be categorised in a manner that some sensitive data would not transfer even to the trusted business partners, and new requirements are elicited, such as "The system shall preserve the customer categorised data for the minimum amount of time to support the business purpose and to meet the legal compliance" to ensure security and privacy goals.

4. Related Work

Mouratidis et al. [4] presented Secure Tropos for eliciting security requirements in terms of security constraints and the approach of Islam [8] extended it with security attack scenarios, where possible attackers, their attacks, and system resources are modelled. Islam [8] also proposed a goal-based software development risk management model (GSRM) to assess and manage risks from the RE phase. Antón et al. [1] introduce two classes of privacy related software requirements through two classes: privacy protection goals such as integrity & security and privacy harms based on vulnerabilities relating to information monitoring, aggregation, storage, transfer, collection, and personalization. Breaux et al. [10] consider activity, purpose, and rule sets to extract rights, obligations, and constraints from legal texts. Ghanavati et al. [7] use User Requirement Notation based on Goal-oriented Requirement Language for a requirement management framework by modelling hospital business

process and privacy legislation in terms of goals, tasks, actors, and responsibilities. Siena et al. [2] focus on Hohfeld's legal taxonomy and map the legal rights with the i* goal modelling language to extract legal compliance requirement. In [8], we use Secure Tropos to model regulation, based on Hohfeld's legal taxonomy, in order to extract requirements that comply with legislation.

As foundation for our work we use SecureTropos, GSRM, activity and purpose patterns, and rule sets. Our framework contributes that it enables the analysis of privacy regulations beyond the only permitted and required actions and it facilitates the consideration of non-compliance issues and risk management since the early stages of the development process. Furthermore, it supports adopting security and privacy requirements to a change of legislation.

5. Conclusion

Security and privacy practices are important for software that manages sensitive information and for stakeholders when selecting software or service providers to serve their business needs. Therefore, organisations responsible to manage sensitive data cannot escape the obligation to implement the requirements established by privacy regulations and changes therein. This paper advances the current state of the art by contributing the foundations of a framework that aligns security and privacy requirements with relevant legislation.

References

[1] A. Antón, J. Earp, and A. Reese. Analyzing website privacy requirements using privacy goal taxonomy. Proc. of the IEEE Joint International Conference on RE, pp. 23–31, 2002.

[2] A. Siena, J. Mylopoulos, A. Perini and A. Susi, Towards a framework for law-compliant software requirements, Proc. of the 31st International Conference on Software Engineering (ICSE09), Vancouver, Canada.

[3] Bundesdatenschutzgesetz - Federal Data Protection Act (as of 15 November 2006).

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

[5] 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.

[6] Information society, Summary of legislation, European Commission.

[7] S. Ghanavati , D. Amyot and L. Peyton, A Requirements Management Framework for Privacy Compliance, Workshop on Requirements Engineering (WER07),Toronto,Canada.

[8] S. Islam, Software development risk management model: a goal driven approach, Proceedings of the doctoral symposium for ESEC/FSE on Doctoral symposium, 2009, Amsterdam, The Netherlands.

[9] S. Islam, H. Mouratidis, J.Jürjens, A Framework to Support Alignment of Secure Software Engineering with Legal Regulations, to appear Journal of Software and Systems Modeling (SoSyM) Theme Section NFPinDSML, DOI : 10.1007/s10270-010-0154-z, 2010.

[10] T. D, Breaux and A. I. Antón, Analyzing Regulator Rules for privacy and Security Requirements, IEEE transactions on software engineering, Vol. 34(1) Jan-Feb 2008.

[11] W. N. Hohfeld, fundamental Legal Conceptions as Applied in Judicial Reasoning, Yale Law of Journal 23(1), 1913.