Supporting Model-based Privacy Analysis by Exploiting Privacy Level Agreements

Amir Shayan Ahmadian[1], Jan Jürjens[1,2]
[1] Institute for Software Technology, University of Koblenz-Landau, Germany, ahmadian@uni-koblenz.de
[2] Fraunhofer-Institute for Software and Systems Engineering ISST, Dortmund, Germany, http://jan.jurjens.de

***Abstract*—Security and privacy are increasing concerns for both IT service customers and providers. According to cloud security alliance (CSA), privacy level agreements (PLAs) are intended to be used as appendixes to service level agreements and are likely to become as an industry standardized way for cloud service providers to describe the level of privacy and data protection. In this paper, we introduce an approach to verify whether the system design of a service provider supports the service customer's privacy and security preferences, by exploiting PLAs. In the first step, we formalize the PLAs. To this end, a metamodel for the PLAs is provided. This metamodel is based on the PLA outline provided by CSA, which is originally based on Directive 95/46/EC. In our research, we first investigate if an adaptation of the PLA outline with respect to the Regulation 2016/679 (repealing of Directive 95/46/EC) on the protection of natural persons with respect to the processing of personal data, is required. Afterwards, we describe how the PLAs are used to support model-based privacy and security analyses. Moreover, we explain how the analyses results can be used to refine PLAs. Our approach is supported by the CARiSMA tool. To evaluate the approach, we applied it to a real industry case study.**

I. Introduction

A main problem for the IT companies that process personal data of the customers and the employees is to provide data protection, security, and avoid data breaches. According to a global survey [1], 88% of people are concerned about who can access their private data. In Germany, 72% of consumers expect the government to keep out of their personal data. The development and the use of new technologies and business models such as cloud computing and open government have even increased the complexity of ensuring security and data privacy extensively.

The service customers need to know if the level of privacy, and security are fulfilled according to the legal basis and their own privacy and security preferences. Besides, the IT service providers need to convince their customers of security and data privacy.

In our research, we provide an approach to verify whether the system design of a service provider supports the service customer's preferences concerning privacy and security, by exploiting privacy level agreements (PLAs). PLAs provide a structured way to precisely specify the level of privacy and personal data protection that the service providers offer to maintain with respect to the related data processing [2]. In the course of our research project VisiOn [3], we extended the PLA outline (provided by Cloud Security Alliance [4]) to capture the privacy and security preferences of the service customers and subsequently perform privacy and security analyses to verify if the preferences are supported concerning the system design of the services.

9781-5090-1445-3/16$31.00

Model-based techniques provide a possibility to support privacy and security analyses. Using the system models, the privacy requirements are considered from early stages of the design and the development process. Motivated by this, we investigate the following research questions:

- RQ1: How can privacy level agreements (PLAs) be formalized to support model based privacy analysis?
- RQ2: How can we verify if the privacy and security preferences that are specified in the PLAs are supported by the system design?

The rest of this paper is organized as follows. Section II provides a brief background on model based security analysis (UMLsec). Section III presents the formalized Privacy Level Agreement. Section IV briefly introduces the main concepts of our approach. Section V introduces the case study. In Section VI, we provide the related work. Finally in Section VII, we provide a conclusion.

II. Background

UMLsec [5], [6] provides an approach to develop and analyze security critical software, in which security requirements such as integrity, availability, and confidentiality are presented in system models (modeled by UML diagrams [7]). The UMLsec language is an UML profile (a lightweight extension of UML using the standard UML extension mechanisms), which can be easily annotated in existing UML tools and thus easily be integrated into the development, without breaking existing processes. Security requirements are expressed using, stereotypes and tags. The main idea of UMLsec is to present maximal analysis power, while allowing to use everyday development tools. UMLsec provides so called checks to ensure the annotated requirements. The CARiSMA tool [8], [9] can be used for the relevant security analysis. UMLsec has been used to investigate a variety of security properties (such as [10]) in a number of applications in practice (such as [11], [12], [13], [14], [15]). The relation to other non-functional requirements has been investigated e.g. in [16] and recently the security analysis techniques have also been applied at the code level [17] and integrated with the requirements elicitation phase [18], [19].

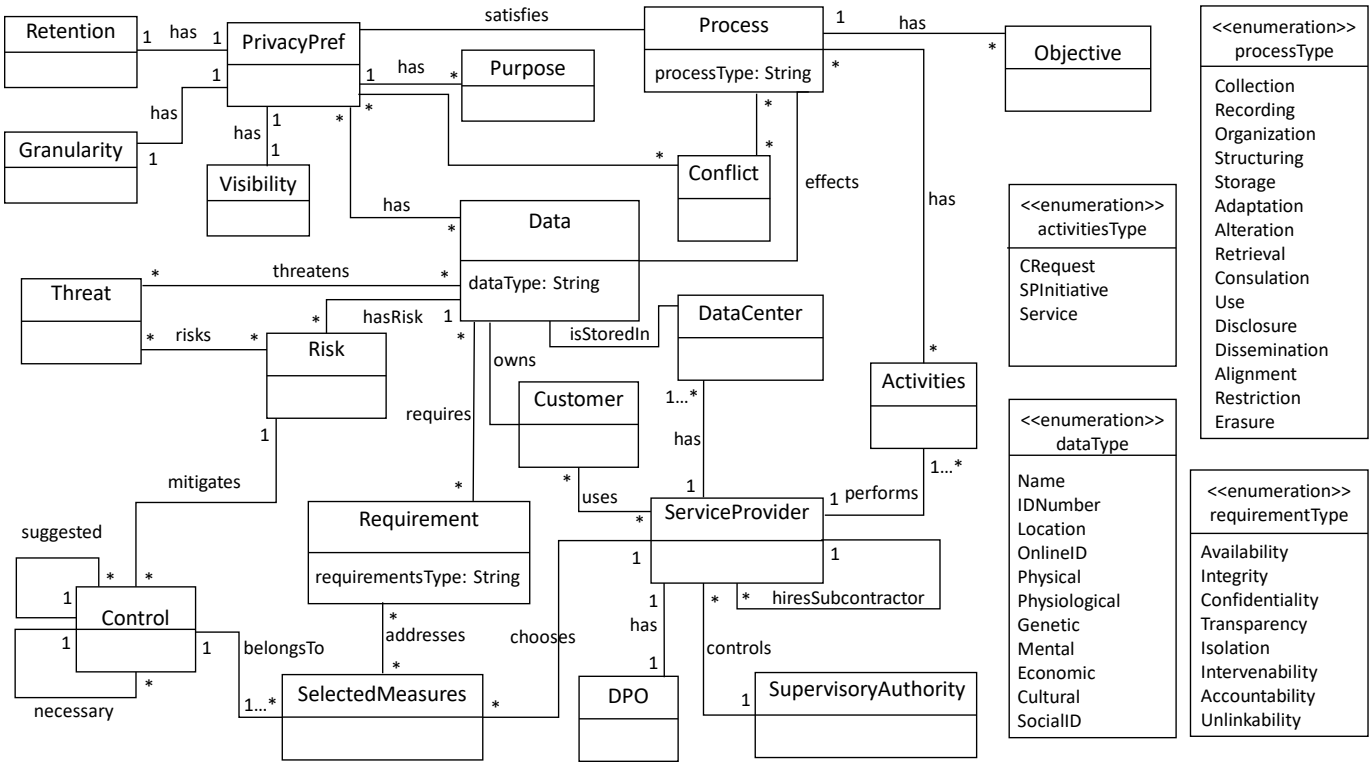

Fig. 1. The PLA metamodel.

III. Formalized Privacy Level Agreements: The PLA Metamodel

In order to support the model-based privacy analysis by exploiting PLAs, a formal description of the PLAs is required. Figure 1 provides the metamodel to express the PLAs. The textual PLA outline [2] (provided by CSA) consists of different sections. The metamodel (Figure 1) manifests all these sections.

According to the PLA outline [2], many concepts are driven from *Directive 95/46/EC* [20] of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data. On 27 April 2016, *Regulation (EU) 2016/679* (General Data Protection Regulation, or *GDPR*) on the protection of natural persons with regard to the processing of personal data and on the free movement of such data [21] is provided by the European Parliament. *Regulation (EU) 2016/679* repeals *Directive 95/46/EC*. Therefore, before modeling the PLA metamodel, we compared *Regulation (EU) 2016/679* with *Directive 95/46/EC* to update and extend the PLA outline to be compliant with *Regulation (EU) 2016/679*. Due to the lack of space, this comparison and the adaptation of the PLA outline cannot be provided in this paper.

GDPR adds some new definitions, updates some of the basic principles, and formulates some new principles. From the 99 Articles contained in *GDPR*, 26 Articles are not directly mentioned or contained in *Directive 95/46/EC*. 37 Articles are updated, or are described in a more comprehensive manner. For instance, in Article 4, new definitions such as genetic and biometric data, profiling, and pseudonymisation are added. In Article 25 the idea of *data protection by design and default* is provided, which is not contained in *Directive 95/46/EC*.

Although *Regulation (EU) 2016/679* shall apply from 25 May 2018, we considered this regulation as a basis for modeling the PLA metamodel. The terms and names that are used in the metamodel are based on terms and definitions of *Regulation (EU) 2016/679*.

Due to the lack of space, this metamodel is simplified, and the relevant attributes and the methods are not presented. Moreover, some of the concepts which are contained in the PLA outline are not expressed in this metamodel since they are not required for the privacy/security analysis. For instance, the *Employee* or *Auditor* classes are not contained in this metamodel.

Each service customer owns its private data, which will be stored in the data center of the service provider and will be processed through different activities (processes) that the service provider presents. According to the PLA outline, the service provider could be a controller, a processor, or a joint controller. The activities could be the services (e.g. storage of data), the customer's requests (e.g. report preparation), or the service provider initiative (e.g. back-up, fraud monitoring). Different types of the processes and the data are provided as enumerations. For the data types, in addition to the data types that are contained in the PLA outline, the types that are defined in *Regulation (EU) 2016/679* are included.

Each data has privacy preferences. The privacy preferences of the service customer simply specify the desired privacy requirements of the customer concerning the provided personal data. The privacy preferences are based on the four key elements of privacy provided in [22]. In what follows, the four elements of privacy preferences are provided and briefly described:

- Purpose: Purpose is the fundamental element of data privacy. It specifies the legitimate reasons to access a specific piece of data [23]. The service customers have different motivations for providing data to the service providers. The service providers must explicitly record and track the purposes for which the data is collected.
- Retention: According to the legal requirements, the data must be collected for limited purposes and it should be removed or restricted after it has been used for the intended purposes. Therefore, a privacy definition must include a retention period for the data, and the service provider must respectively provide a mechanism to remove or restrict the data.
- Visibility: It indicates who is allowed to access or use data provided by the service customer for an authorized purpose. In other words, visibility restricts the number of users who can access data regarding an operation and a purpose.
- Granularity: It refers to characteristics of data that could be used to facilitate proper use of the data, where there exists different valid accesses for various purposes. In other words, data granularity describes how much accuracy is provided in response a query. It becomes useful when the service customer requires the service provider to provide personal data to a third party [23].

The privacy preferences are specified by the service customer. Additionally, for each process a set of objectives are defined, which describes the purposes of the processes or indicates if the process restricts or deletes the data that is processed. The privacy preferences will be later used as the input of the privacy and security analyses to investigate if they are satisfied by the system design, i.e. they are compared against the objectives of the processes. The possible conflicts between the privacy preferences of the service customer and the services are defined in the conflict class. In Section IV, we will briefly describe how the conflicts are identified and how they are handled.

Article 35 of *Regulation (EU) 2016/679* refers to *data protection impact assessment*. This requires carrying out an assessment of the impact of the envisaged processing operations on the protection of personal data [21]. Therefore, in the metamodel threats, risks, privacy/security requirements are included.

Moreover as we mentioned previously, Article 25 of *Regulation (EU) 2016/679* refers to *data protection by design and default*. This requires that the service providers implement appropriate technical and organizational controls in an effective manner, and integrate proper safeguards into the processing.

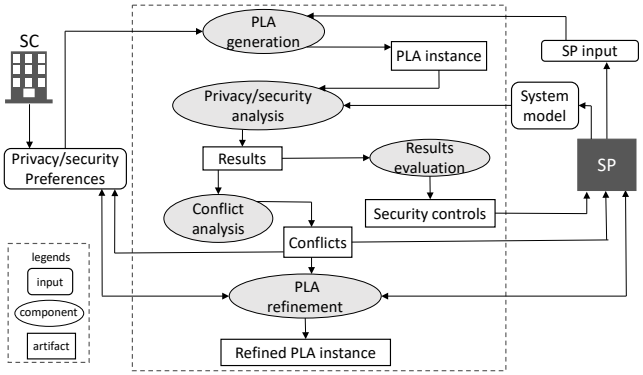

Fig. 2. Overview of the proposed approach.

The implementation of the security and privacy controls are also mentioned in the PLA outline [2] (Section 4). Thus, we include the controls and the selected measures in the PLA metamodel. As a part of our approach, and based on the results of the security and privacy analyses, and the calculated risks, appropriate measures and mechanisms will be recommended to the service providers to ensure data privacy and security.

Furthermore, for each service provider a data protection officer (DPO) and a supervisory authority is defined. The specification of the DPO refers to Article 37 of *Regulation (EU) 2016/679* and Section 1 of the PLA outline. The specification of the supervisory authority refers to Article 51 of *Regulation (EU) 2016/679* and Section 6 of the PLA outline.

In the following section, we briefly describe how the PLA will support privacy and security analyses.

IV. Supporting Model-based Privacy Analysis Using PLAs

Figure 2 demonstrates the overview of our approach. The service customer (SC) indicates the privacy and security preferences. The process of identifying the preferences is performed using a simple questionnaire. The service customer specifies the privacy preferences of the provided personal data, i.e. indicates the allowed purposes of the process, the retention time that the data will be stored in the data center of the service provider, who is allowed to process or access the data (visibility), and the characteristics of the data (granularity). The privacy preferences are automatically included in the PLA instance (an instantiated class diagram) during the PLA generation.

The service provider delivers the system model (modeled using UML diagrams) that specifies the structure and the behavior of the system. Moreover, the provider delivers other useful information such as the supervisory authority and the data protection officer, which are inserted in the PLA instance.

The system model and the PLA instance are given to the security and privacy analysis component. In our approach we use CARiSMA to perform security analysis. CARiSMA provides the possibility to perform security analysis to verify whether the security requirements are supported by the system design. CARiSMA includes different security checks.

As we mentioned in Section II, the underlying concept of CARiSMA is UMLsec. UMLsec originally includes different stereotypes and tags to annotate the UML diagrams with the security requirements. In our research, favoring UMLsec profile, we develop a privacy analysis approach to support the privacy requirements. We implement this approach by extending CARiSMA with respective privacy analysis checks. This approach is based on the four key technical dimensions to privacy (purpose, visibility, granularity, and retention) [22]. Article 5 of *Regulation (EU) 2016/679* on *principles relating to processing of personal data* also explicitly refers to these four dimensions.

In a nutshell, the privacy analysis approach that is introduced in this paper provides a possibility to analyze the system design of the service provider concerning the four key privacy dimensions, and in a model based approach investigate if the privacy preferences of the service customer are supported. In what follows, we briefly describe how this analysis is performed.

To verify if the allowed purposes that are indicated by the customer for the personal data are supported by the system design, the purposes of the personal data that are included in the privacy preferences are compared against the objectives of the services. A service contains different components, and the structure of each component comprises different classes, which is demonstrated as a UML class diagram. For each class in the class diagram a set of operations are specified. Using the privacy profile that is created for the privacy analysis approach, the objectives of the operations, which indicates the purposes of the operations are specified. After collecting all the objectives of the operations contained in the different classes, it is possible to identify the objectives of the service that processes the personal data. The purposes of the personal data (contained in the privacy preferences) are compared with these objectives. If there exists any conflicts between the allowed purposes and the objectives of the service, the privacy check that is relevant to the purposes fails and the results will be documented. The whole process described above is performed automatically.

Similarly, the operations that remove or restrict the data are annotated with relevant stereotypes from the privacy profile. In this way, the system design of the service is verified to check if an appropriate operation exists that removes or restricts the personal data concerning the retention period. It is possible to define a retention for a specific purpose, i.e. after exceeding the retention period, the personal data must not be processed regarding the given purpose. Moreover, according to Article 9 of *Regulation (EU) 2016/679* on *notification obligation regarding rectification or erasure of personal data or restriction of processing*, the service provider must inform the service customer about removing or restricting of the personal data. Concerning the system design of the service provider (models), by analyzing the behavior of the service provider (for instance, analyzing the UML sequence diagram), it is possible to verify if the service customer is informed about the erasure or restriction of the personal data.

To check the visibility, our approach extends the RBAC (role-based access control [24]) check of UMLsec [5], and provides the RABAC check (role attribute-based access control [25]). Originally, RBAC check is used to enforce role-based access control in the business process specified in the activity diagram [5]. In our approach, in addition to the roles and the roles hierarchy that is defined for the data subjects, the analysis and the access to the data is also based on the attributes of the data. For instance, the location of the data could be defined as a critical attribute, which must be explicitly considered in the analysis. In this way, for example the access to data is given to a person from a specific public organization but not to a private organization. These specifications are contained and annotated in the system design. Particularly, UML class diagrams and activity diagrams are used for the specification (annotation), and the analysis. During the analysis, the system model is compared with the privacy preferences (visibility) that are specified by the service customer.

The level of the granularity is analyzed together with the specific purpose, i.e. the level of granularity that is contained in the privacy preferences implies that the service and its relevant operations are only allowed to process the data concerning the given level.

The work presented in this paper is in progress, and we are moving towards more comprehensive mechanisms to automatically analyze the privacy preferences of the customers, and complete and formalize the concepts that are provided in this section.

After performing privacy and security checks, using the results of the respective analyses, appropriate privacy and security measures and mechanisms will be recommended to the service provider to ensure security and privacy of the services. To this end, we use the results of our previous work [26], in which a workflow to support small and medium-sized enterprises in the cloud system certification process based on ISO 27001 [27] is provided. One of the main result of this workflow was a security measure list to mitigate the identified risks during the risk analysis process. In our current work, we extended this measure list with appropriate measures and mechanisms to support privacy requirements. For instance, if the result of the security analysis indicates that the confidentiality of a link that transmits the personal data is not properly provided, then the service provider may be recommended to use an encrypted link to transmit the personal data.

Moreover, the results of the security and privacy analysis component and the identified conflicts between the customer's preferences and the system design are delivered to the conflict analysis component. This component analyzes the results and the conflicts and provides a mechanism to handle the conflicts. The results of this component are documented in the PLA instance. For instance, if there is any conflict between the purposes that are specified for the personal data (indicated by the service customer), and the objectives of the process that are specified in the system design, either the service provider must avoid processing the personal data regarding the prohibited

purpose or the customer must accept that the personal data will be used for that purpose.

Finally, the refined PLA instance containing different information such as privacy preferences of the service customer concerning the conflicts, and appropriate privacy and security measures and mechanisms is generated.

V. Case Study

To evaluate our approach we applied it to a real industry case study, namely a birth certificate registration process in the Municipality of Athens. This is a case study from the VisiOn project [3], in which the privacy level of a public administration system is evaluated and a privacy level agreement between a customer and the public administration will be generated.

Municipality of Athens (MoA) is a Public Administrator (PA) in Athens. MoA develops a new system MACS (Municipality Athens Citizen System), which stores all the customer's data. MACS provides different online services to the customers.

One of the services is issuing a birth certificate for a customer. In this process, the customer provides an application form to the MACS. This application form contains different data such as, citizen's ID number, the phone number, the address, and the birth information.

To analyze the privacy of the MACS's system design, in the first step, the privacy preferences of the service customers are required. Therefore, before starting the system analysis, using a simple questionnaire, the customer privacy preferences containing allowed purposes, retention time, visibility, and granularity of the personal data are collected. These preferences must not necessarily be specified by the service customer, but could be derived from legal privacy requirements. This process will not take place whenever the customer wants to issue a birth certificate, but only to analyze the system's privacy and for instance, assist the system developer to ensure privacy and security in MACS during the design time. The customer may require that the personal data must not be used for commercial purposes, specifies that the given personal data must be deleted in one year after issuing the birth certificate, and only the administrator of the MACS in the citizen registry department is allowed to read the data. This information are included in the PLA instance of the customer.

Issuing a birth certificate as a service is modeled using UML diagrams (deployment, sequence, component, activity, and class diagram). This service contains different classes with different operations. The operations are *getAppForm()*, *issueBirthCertificate()*, *saveAndClose()*, for which a set of purposes are specified. This set of purposes are compared with the allowed purposes that are indicated by the customer. In case of any conflict, the results will be documented in the PLA, and the customer will be informed. Moreover, appropriate privacy and security measures and mechanisms will be recommended to the service provider (MoA).

In this case study in total, we analyzed three different scenarios of MoA including three different services. Results include that our approach can be successfully applied to a real industry case study with complex services, processes, and components. Specifically, according to the two research questions investigated in this work, results include the following:

- RQ1: We provided a metamodel to formalize the privacy level agreements in order to support model based privacy analysis. We considered *Regulation (EU) 2016/679* as a basis for modeling the PLA metamodel. The PLA instance for each service customer that is modeled as a class diagram, contains the privacy preferences of the customer.
- RQ2: We provided a privacy package based on the four key elements of the privacy (purpose, retention, visibility, and granularity), and implemented our approach by extending CARiSMA in order to perform privacy analysis. The privacy and security preferences of a service customer are captured in a PLA, and using CARiSMA, automatically the system design of the service provider is analyzed to verify whether the privacy and security requirements are supported.

VI. Related Work

We are aware of only one published work on formalization of the PLA. In this work [28], the authors propose an ontology-based model to represent the information included in the privacy level agreements and automate the process of enforceable policy creation. Moreover they extend this ontology to create a link between policy elements in the PLA and the actual policies processed by software systems. The ontology that they provide establishes a mapping between high level policies and low level policies (machine readable policies). However in our work, we use the PLA metamodel to support the privacy analysis of the IT systems. Furthermore, our PLA metamodel is based on the Regulation 2016/679.

In [29], a framework is provided to support the elicitation and analysis of security requirements from relevant regulations and laws, and develop a system that satisfies these requirements. In their work, they also use UMLsec to support the development of a design to satisfy the elicited security requirements. However, they do not support the elicitation of the service customer's security and privacy preferences and the analysis of the system design based on these preferences.

In [30], a framework for model based privacy 'best practice' compliance checker that assists the experts to reason about how privacy compliance may be satisfied, optionally using predefined models, is introduced. In their work, they consider top level security and privacy goals, and link them to the system level enforcement technologies. They do not focus on the system design and they do not perform an analysis on the architecture of the services.

In [31], the authors argue that the privacy must be considered when cloud computing services are designed, and it should be built into every stage of the product development process. They have suggested a variety of guidelines and techniques to assist the software engineers to achieve this.

VII. Conclusion

In this paper, we introduced an approach, to support the service customers to verify if their privacy and security preferences are supported by the system design, using privacy level agreements. Moreover, in this approach we assist the service providers to convince the customers of the security and privacy, by recommending appropriate security and privacy mechanisms, and handling the conflicts between the customer's preferences and the system design. This approach is suitable for both designing new services (privacy by design) and analyzing the privacy of the existing services (privacy analysis). Our approach only focuses on the design of the system, and generate a PLA containing the privacy preferences of the service customer and the system specification together with the results of the analysis, appropriate measures and mechanisms, and possible conflicts between the design of the system and customer's requirements. This approach is integrated into VisiOn project, in which different tools are integrated to provide a platform to privacy and security analysis of public administration systems. The VisiOn privacy platform provides the possibility to enforce privacy level agreements during runtime.

ACKNOWLEDGEMENTS

This research was partially supported by the research project Visual Privacy Management in User Centric Open Environments (supported by the EU's Horizon 2020 program, Proposal number: 653642).

References

[1] Fujitso Research Institute, "Personal data in the cloud: The importance of trust," Tokyo 105-7123, JAPAN, Sep. 2010.

[2] Cloud Security Alliance, "Privacy Level Agreement [V2]: A compliance tool for providing cloud services in the european union," https://cloudsecurityalliance.org/download/privacy-level-agreement-version-2, 2009.

[3] (2016) VisiOn Project. [Online]. Available: http://www.visioneuproject.eu/

[4] Cloud Security Alliance. Accessed: 2016-08-07. [Online]. Available: http://cloudsecurityalliance.org/

[5] J. Jürjens, *Secure systems development with UML*. Springer, 2005. [Online]. Available: http://dx.doi.org/10.1007/b137706

[6] J. Jürjens, "Model-based security engineering with UML," in *Foundations of Security Analysis and Desing III: FOSAD 2004/2005 Tutorial Lectures*, ser. Lecture Notes in Computer Science, A. Aldini, R. Gorrieri, and F. Martinelli, Eds., 2005, vol. 3655, pp. 42–77.

[7] Object Management Group (OMG), "UML 2.4.1 Superstructure Specification," 2011.

[8] S. Höhn and J. Jürjens, "Rubacon: Automated support for model-based compliance engineering," in *International Conference on Software Engineering (ICSE)*. ACM, 2008, pp. 875–878.

[9] (2016, May) CARiSMA. [Online]. Available: https://rgse.uni-koblenz.de/carisma/

[10] J. Jürjens, "Secure information flow for concurrent processes," in *11th International Conference on Concurrency Theory (CONCUR 2000)*, ser. Lecture Notes in Computer Science, vol. 1877. Springer Verlag, 2000, pp. 395–409.

[11] J. Jürjens and G. Wimmel, "Security modelling for electronic commerce: The Common Electronic Purse Specifications," in *First IFIP Conference on e-Commerce, e-Business, and e-Government (I3E)*. Kluwer, 2001, pp. 489–505.

[12] J. Jürjens, "Modelling audit security for smart-card payment schemes with UMLsec," in *16th International Conference on Information Security (IFIPSEC"01)*, IFIP. Kluwer, 2001, pp. 93–108.

[13] J. Jürjens and G. Wimmel, "Formally testing fail-safety of electronic purse protocols," in *16th International Conference on Automated Software Engineering (ASE 2001)*. IEEE, 2001, pp. 408–411.

[14] S. H. Houmb, G. Georg, J. Jürjens, and R. B. France, "An integrated security verification and security solution design trade-off analysis approach," in *Integrating Security and Software Engineering: Advances and Future Vision*, H. Mouratidis, Ed. Idea Group, 2006, pp. 190–219, invited chapter.

[15] E. Fernández-Medina, J. Jürjens, J. Trujillo, and S. Jajodia, "Model-driven development for secure information systems," *Information & Software Technology*, vol. 51, no. 5, pp. 809–814, 2009.

[16] D. Petriu, M. Woodside, D. Petriu, J. Xu, T. Israr, G. Georg, R. France, J. Bieman, S. H. Houmb, and J. Jürjens, "Performance analysis of security aspects in UML models," in *Sixth International Workshop on Software and Performance (WOSP 2007)*. Buenos Aires, Argentina: ACM, 2007, pp. 91–102.

[17] F. Dupressoir, A. D. Gordon, J. Jürjens, and D. Naumann, "Guiding a general-purpose c verifier to prove cryptographic protocols," *Journal of Computer Security*, vol. 22, no. 5, pp. 823–866, 2014, special issue with best papers from the 24th IEEE Computer Security Foundations Symposium (CSF).

[18] R. Breu, K. Burger, M. Hafner, J. Jürjens, G. Popp, G. Wimmel, and V. Lotz, "Key issues of a formally based process model for security engineering," in *Sixteenth International Conference "Software & Systems Engineering & their Applications"*, Paris, 2003.

[19] K. Schneider, E. Knauss, S. Houmb, S. Islam, and J. Jürjens, "Enhancing security requirements engineering by organisational learning," *Requirements Engineering Journal (REJ)*, vol. 17, no. 1, pp. 35–56, 2012.

[20] European Parliament, Council of the European Union, "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data," *Official Journal of the European Union*, vol. L 281, 1995.

[21] European Parliament, "Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data ," *Official Journal of the European Union*, vol. L 119, 2016.

[22] K. Barker, M. Askari, M. Banerjee, K. Ghazinour, B. Mackas, M. Majedi, S. Pun, and A. Williams, "A data privacy taxonomy," in *Dataspace: The Final Frontier, 26th British National Conference on Databases, BNCOD 26, Birmingham, UK, July 7-9, 2009. Proceedings*, 2009, pp. 42–54.

[23] K. Ghazinour, M. Majedi, and K. Barker, "A lattice-based privacy aware access control model," in *Computational Science and Engineering, 2009. CSE '09. International Conference on*, vol. 3, Aug 2009, pp. 154–159.

[24] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, "Role-based access control models," *Computer*, vol. 29, no. 2, pp. 38–47, Feb. 1996. [Online]. Available: http://dx.doi.org/10.1109/2.485845

[25] X. Jin, R. Sandhu, and R. Krishnan, *RABAC: Role-Centric Attribute-Based Access Control*. Springer Berlin Heidelberg, 2012, pp. 84–96. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-33704-8_8

[26] A. S. Ahmadian, F. Coerschulte, and J. Jürjens, *Supporting the Security Certification and Privacy Level Agreements in the Context of Clouds*. Springer International Publishing, 2016, pp. 80–95. [Online]. Available: http://dx.doi.org/10.1007/978-3-319-40512-4_5

[27] "ISO/IEC 27001 Information Security Management System (ISMS) standard," International Organization for Standardization, Geneva, Switzerland, ISO 27001:2013, Oct. 2013.

[28] M. D'Errico and S. Pearson, "Towards a formalised representation for the technical enforcement of privacy level agreements," in *Cloud Engineering (IC2E), 2015 IEEE International Conference on*, March 2015, pp. 422–427.

[29] S. Islam, H. Mouratidis, and J. Jürjens, "A framework to support alignment of secure software engineering with legal regulations," *Software & Systems Modeling*, vol. 10, no. 3, pp. 369–394, 2011. [Online]. Available: http://dx.doi.org/10.1007/s10270-010-0154-z

[30] S. Pearson and D. Allison, "A model-based privacy compliance checker," *IJEBR*, vol. 5, no. 2, pp. 63–83, 2009. [Online]. Available: http://dx.doi.org/10.4018/jebr.2009040104

[31] S. Pearson, "Taking account of privacy when designing cloud computing services," in *Proceedings of the 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing*, ser. CLOUD '09. IEEE Computer Society, 2009, pp. 44–52. [Online]. Available: http://dx.doi.org/10.1109/CLOUD.2009.5071532