Model-Based Privacy and Security Analysis with CARiSMA

Amir Shayan Ahmadian
University of Koblenz Landau, Germany
ahmadian@uni-koblenz.de

Sven Peldszus
University of Koblenz Landau, Germany
speldszus@uni-koblenz.de

Qusai Ramadan
University of Koblenz Landau, Germany
qramadan@uni-koblenz.de

Jan Jürjens
University of Koblenz Landau, Germany
Fraunhofer ISST, Germany
http://jan.jurjens.de

ABSTRACT

We present CARiSMA, a tool that is originally designed to support model-based security analysis of IT systems. In our recent work, we added several new functionalities to CARiSMA to support the privacy of personal data. Moreover, we introduced a mechanism to assist the system designers to perform a CARiSMA analysis by automatically initializing an appropriate CARiSMA analysis concerning security and privacy requirements. The motivation for our work is Article 25 of Regulation (EU) 2016/679, which requires appropriate technical and organizational controls must be implemented for ensuring that, by default, the processing of personal data complies with the principles on processing of personal data. This implies that initially IT systems must be analyzed to verify if such principles are respected. System models allow the system developers to handle the complexity of systems and to focus on key aspects such as privacy and security. CARiSMA is available at (http://carisma.umlsec.de) and our screen cast at (https://youtu.be/b5zeHig3ARw).

CCS CONCEPTS

• **Security and privacy** → *Software security engineering*; • **Software and its engineering** → *Software design engineering*;

KEYWORDS

System design analysis, Model-based analysis, Privacy, Security

ACM Reference format:
Amir Shayan Ahmadian, Sven Peldszus, Qusai Ramadan, and Jan Jürjens. 2017. Model-Based Privacy and Security Analysis with CARiSMA. In *Proceedings of 2017 11th Joint Meeting of the European Software Engineering Conference and the ACM SIGSOFT Symposium on the Foundations of Software Engineering, Paderborn, Germany, September 4–8, 2017 (ESEC/FSE'17),* 5 pages.
https://doi.org/10.1145/3106237.3122823

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.
ESEC/FSE'17, September 4–8, 2017, Paderborn, Germany
© 2017 Copyright held by the owner/author(s). Publication rights licensed to Association for Computing Machinery.
ACM ISBN 978-1-4503-5105-8/17/09…$15.00
https://doi.org/10.1145/3106237.3122823

1 INTRODUCTION

Nowadays, IT service providers increasingly require personal data of their customers to perform their services [27]. For instance, public administrations such as hospitals or administration offices of municipalities are offering more and more IT services to patients and citizens. Such services enormously involve personal data processing. Although these services have many benefits, new security and privacy risks emerge when security and privacy concerns are not appropriately supported during the development process [4].

Article 25 of Regulation (EU) 2016/679 [30] introduces data protection by design. Data protection by design is not a novel concept, and is firstly introduced by Cavoukian [3]. However, earlier – prior to the releasing Regulation (EU) 2016/679 – it lacked a legal incentive to drive its adoption process in the European Union. Data protection by design requires that appropriate technical and organizational measures must be implemented to ensure that, by default, a piece of personal data is processed with respect to the principles on processing of personal data. Such principles, in addition to the legal requirements, include the security and privacy requirements of customers and citizens. Data protection by design implies that in early software development phases, the design of a system must be analyzed regarding the legal requirements and the requirements of service customers, and where necessary the design has to be improved to technically support privacy and security [5, 28].

The CARiSMA tool supports such an analysis in a model-based manner using the UML extension UMLsec [13]. CARiSMA has been designed to support the security analysis of IT systems by providing a set of security checks. System models allow the system designers to handle the complexity of systems and to focus on key aspects such as privacy and security. UMLsec has in particular been used in the context of security requirements analysis [26], combined with the analysis of other non-functional requirements such as performance [25] and applied to practical applications (cf. e.g. [14]). UMLsec and respectively CARiSMA currently do not enable a system designer to express privacy requirements in the design of IT systems.

Despite the fact that CARiSMA enables system designers to express security requirements [8] such as confidentiality, integrity, and availability within system models, annotating the system models properly, and initializing appropriate CARiSMA analysis are challenging processes. CARiSMA provides no automatic mechanism to assist system designers in performing an analysis concerning given security and privacy requirements. In other words, the

system designer has to manually analyze the requirements and perform an appropriate analysis.

The results of an analysis may contain information on weaknesses in a system design. Additional tool support for automated or assisted evaluation of such analysis results may assist a system developer to handle the conflicts between system models and the requirements, or mitigate the risks that have been arisen from the system flaws. However, CARiSMA originally provides no mechanism to support such evaluations.

Based on these considerations, in this work we introduce the following new functionalities for CARiSMA: (I) **Analyzing security and privacy requirements** to automatically initialize analyses and assist system designers with annotating the system models. (II) **Role-attribute-based access control** to support model-based privacy analysis of system models. (III) **Evaluating analysis results** to generate appropriate questions to collect feedback on potential conflicts between system's design, and security and privacy requirements of citizens.

In this work, we explain the extension of CARiSMA with these new functionalities in order to support privacy and the integration of CARiSMA with other tools from the area of requirement engineering. Moreover, concerning a set of privacy and security requirement, we explain how automatically a system designer may perform an appropriate analysis on system models, how a system designer may be assisted to express such requirements within the system models, and evaluate those new functionalities on an industrial case study.

The paper is organized as follows. In Sec. 2, we provide background and explain new functionalities. In Sec. 3, we apply CARiSMA to an industrial case study. In Sec. 4, we describe how the new functionalities are implemented and integrated into CARiSMA. In Sec. 5, we discuss related work. In Sec. 6, we conclude.

2 OVERVIEW AND NEW FEATURES

Figure 1 demonstrates how CARiSMA is extended to support a system designer with annotating a system model, and to automatically perform an analysis with respect to a set of security and privacy requirements. Given a UML system model as well as security and privacy requirements, first, a system designer performs a pre-analysis. The results of this pre-analysis are: (I) **Configuration data** that automatically initializes a CARiSMA analysis which includes a set of privacy and security checks to analyze the system model concerning the given requirements. (II) **A help report** that assists a system designer to express the security and privacy requirements within system models. Using the help report, a system designer annotates a system model with the security and privacy requirements, and eventually runs the initialized CARiSMA analysis to analyze the system model.

The analysis is based on CARiSMA's original security checks and four new privacy checks. The underlying concepts of the four privacy checks (theoretically introduced in [1]) are the four key privacy elements, namely *purpose*, *visibility*, *granularity*, and *retention*. These privacy elements are introduced in [2], and corresponds to the six principles prescribed in Article 5 of Regulation (EU) 2016/679 [30], for processing of personal data. In a nutshell, by using these privacy checks, it can be verified if: (I) A piece of sensitive data

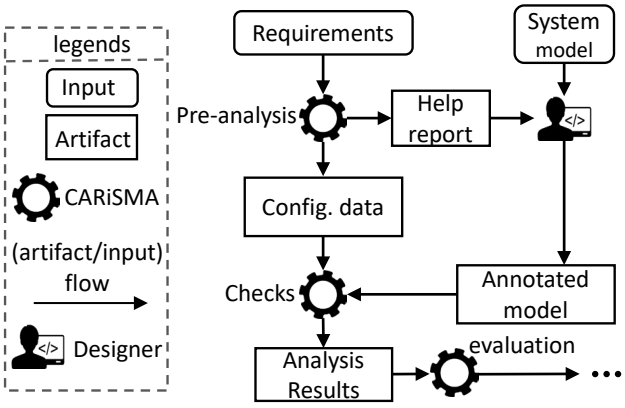

Figure 1: Model-based security and privacy analysis.

is only processed for a set of specific, and legitimate purposes (*purpose-check*). (II) The access to the sensitive data is restricted to authorized persons (*visibility-check*). (III) A piece of sensitive data is legitimately disclosed to other recipients (*granularity-check*). (IV) An appropriate mechanism exits to ensure that sensitive data will be eventually deleted or restricted (*retention-check*). The terms that are used above such as sensitive data or recipient are based on the terms and definitions of Regulation (EU) 2016/679.

The analysis results of such checks can be further evaluated afterwards – e.g. for the generation of privacy related questions. In the context of a case study in the following section, we explain how such evaluations may be performed.

3 SECURITY AND PRIVACY ANALYSIS

We introduce our case study, and briefly demonstrate the security and privacy analysis of our case study with CARiSMA.

3.1 Case Study

The case study discussed in this work and presented in our screencast is one of the case studies of the *VisiOn* EU project (http://www.visioneuproject.eu/), in which a platform for evaluating and analyzing privacy levels of a *public administration* (PA) system is developed. Furthermore, this platform is used to generate agreements on the use of personal data between a citizen and PAs to enforce privacy policies.

The case study is based on a *birth certificate registration* scenario in Municipality of Athens (MoA), a PA in Athens. MoA is in the process of developing a new system called MACS which shall provide different online services to citizens, such as issuing a birth certificate. To provide such services, MoA requires citizen's personal data such as their *Registry Number of Social Insurance* (*AMKA*).

Figure 2 presents an excerpt of the *VisiOn Privacy Platform (VPP)* architecture consisting of three components. (I) **Privacy assessment component** provides a questionnaire to collect the privacy and security requirements of citizens. (II) **Privacy requirement component** specifies and models privacy requirements. (III) **Privacy analysis component** analyzes the system model of a PA.

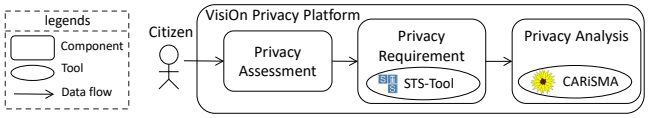

Figure 2: An excerpt from the architecture of VisiOn Privacy Platform (VPP).

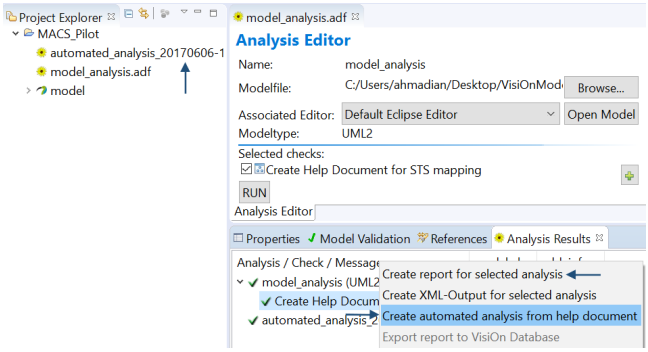

Figure 3: An excerpt from CARiSMA showing the pre-analysis, and the automatically generated analysis.

CARiSMA is integrated into the privacy analysis component, to verify if a PA system supports security and privacy requirements derived from citizen's preferences and legal requirements.

In VPP, the results of the questionnaires, i.e. the output of privacy assessment component, are modeled with the security requirements modeling tool *STS* [21, 22]. A STS model specifies the security and privacy requirements of a PA system. According to Figure 2, STS is integrated into the privacy requirement component. STS models are stored in a central database (called VisiOn database) and may be transferred to other tools in the VPP such as CARiSMA for further analysis. In what follows, we demonstrate how the STS models are analyzed by CARiSMA.

3.2 System Model Analysis Using CARiSMA

Initially a PA system designer or a PA administrator, using the STS tool, models the security and privacy requirements obtained by an assessment tool and store them in the VisiOn database. Afterwards, using CARiSMA different privacy and security analyses are performed to verify a system model concerning the STS models.

MACS's system model is either already modeled by the system designer or exists as a part of system specification. In the first step, the pre-analysis of CARiSMA must be performed on MACS's model. CARiSMA provides an option to automatically read the STS models from the VisiOn database or a local file, and perform the pre-analysis. Figure 3 demonstrates the pre-analysis (*Create Help Document for STS mapping*). After running the pre-analysis, in CARiSMA's results view, different options are provided. A *help report* may be produced, which assists a system designer or a PA administrator with annotating the system models. Moreover, a CARiSMA analysis that contains appropriate security and privacy checks may be automatically generated.

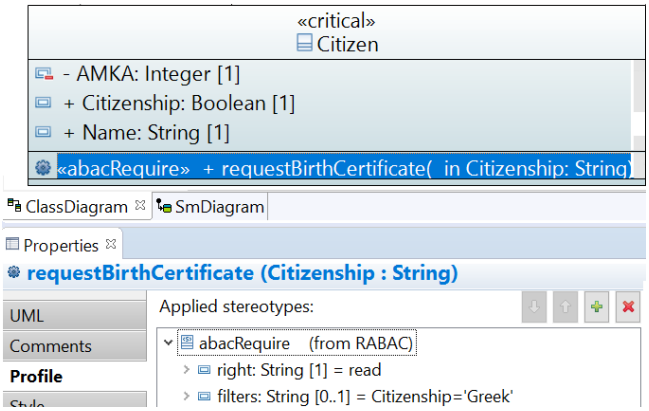

Figure 4: An excerpt from CARiSMA showing the annotation of a class from MACS system with the privacy profile.

A system designer or a PA administrator leverages the produced help report to apply appropriate UML profiles (e.g. the UMLsec or privacy profiles) and stereotypes defined in this profiles to corresponding model elements. Two profiles are introduced in our recent work [1]: (I) The *privacy* profile, which provides a set of stereotypes to annotate UML model elements with privacy specific information. (II) The *rabac* profile, which allows the generation and enforcement of access control policies for system model elements, using the *role- and attribute based access control* model (RABAC [12]).

Figure 4 shows how a class and an operation from a class diagram of the MACS system are annotated with the security and privacy stereotypes *«critical»* and *«abacRequire»*. These annotations particularly enable the visibility-check to perform privacy analysis.

The results of an analysis include detected security and privacy flaws. Different actions may be performed on such analysis results. For instance, in the context of the VPP, the analysis results are contained in the agreements, that are concluded between citizens and PAs on the use of the personal data of the citizens. Moreover, out of such analysis results a set of privacy and security centric questions may be generated. Such questions can be included in the questionnaires to obtain privacy and security preferences of citizens within the privacy assessment component (see Figure 2).

3.3 Discussion

In the course VisiOn project, we applied our analysis to two other public administrations, namely a consortium of two hospitals in Rom and Madrid, and the Italian Ministry of Economic Development (MISE). The models from our case study represent abstractly our partners systems and focus on specific tasks as well as inter system communication. Table 1 shows statistics on the size of the UML models, and the number of security and privacy annotations.

Although the models used in our case study are highly abstracted from the real systems, the evaluation has shown that this level of abstraction enables the system developers to express the security and privacy requirements properly in the models and eventually perform the analysis. However, such models may be expanded with more details for other purposes, without obstructing the privacy and security analysis. In fact the pre-analysis mechanism that is

Table 1: Statistics on the UML Models of our case studies

Institution	model elements	annotations
MoA	141	33
Hospitals	167	31
MISE	309	57

introduced in this paper, facilitates the analysis of large system models such as the models that are obtained using reverse engineering from source code, by generating help reports and initializing appropriate CARiSMA analysis.

Model-based techniques assist developers to handle the complexity of systems by abstractions, allowing them to focus on key aspects of systems such as privacy and security. Although not all the privacy and security issues may be solved by applying model-based techniques, using CARiSMA the privacy and security issues are supported early in the system design. This assists the system implementers to consider and support privacy and security issues in their implementation. In future works, we are going to bridge the gap between the design phase and the implementation phase by synchronizing UMLsec models with the source code. We plan to integrate CARiSMA with the static anti-pattern detection tool HULK [24], and derive security-anti-patterns from UMLsec models.

Having a system model does not imply that the code of the system completely conforms to the models. Therefore, analyzing a system model does not guarantee that the security and privacy requirements are completely supported in the code of the system. Using reverse engineering, the code of a system may be transformed to a system model on which privacy and security requirements may be added and analysis can be performed.

To perform a CARiSMA analysis, the system models must be available in UML. In case different modeling languages are used, one can make use of transformation techniques to transform the models to UML.

4 IMPLEMENTATION AND AVAILABILITY

The CARiSMA tool suite is based on the Eclipse IDE and consists of several components. We contribute the presented new functionalities to the *Profiles* and *Checks* components of CARiSMA and add a new *VisiOn* component for the integration with the other tools in the *VisiOn* privacy platform.

The *Profiles* component contains the specifications of the relevant security and privacy profiles, and registers them at two external components, namely *Papyrus*, and *EMF* model registry. Papyrus is used to model the systems. However, CARiSMA is able to work on any EMF-based UML model. EMF stands for the Eclipse Modeling Framework [29], which is a standard in the Eclipse community for defining models and widely used by different tools. Thus, we additionally register the UML profiles at the EMF model registry. This allows a usage of the UML profiles, for instance, in model transformation tools or with EMF based OCL [20] implementations. The *privacy*, *rabac*, and *UMLsec* profiles enable different security and privacy checks, which are implemented in a *Checks* component.

The *VisiOn* component provides interfaces to the other tools such as STS. The integration with STS is enabled by the VisiOn database. The component is connected to *VisiOn database* component, which is accessed over a *RestAPI*. STS models are stored in this database and CARiSMA retrieve these models from the database and perform a pre-analysis (see Section 3.2).

CARiSMA is published under the Eclipse Public License (EPL) and may be installed from our update-site (http://carisma.umlsec.de/updatesite). Additional help content such as installation instructions and screen casts are available on the CARiSMA website (http://carisma.umlsec.de).

5 RELATED WORK

There are several approaches to support model-based security analysis. Some of those are summarized and discussed by Lano et al. [16]. The model-based use of security patterns has been addressed by some research [15, 19]. Further research makes use of aspect-oriented modeling for model-based security [7]. Heitmeyer et al. propose the application of formal methods on minimal state machine models for security verification [9].

SecureUML provides a role-based access control using UML models [17]. While CARiSMA provides interfaces for adding arbitrary profiles and checks, SecureUML is limited to access control.

The CORAS tool provides security risk analysis [6]. CORAS works on proprietary models and uses the CORAS language, which was a UML profile but later defined as a domain specific language.

In VisiOn project, two tools namely, SecTro, and JTrust are integrated within the requirement analysis component to provide security thread analysis. SecTro is built upon the Secure Tropos approach and is used to model security during requirements engineering [18, 23]. JTrust evaluates the trustworthiness of a system based on trust and control models [11].

Islam et al. integrated the Secure Tropos approach with UMLsec, to support the alignment of secure software engineering with legal regulations [10]. However, this work does not support privacy requirements and they do not analyze security requirements to automatically perform appropriate UMLsec checks.

6 CONCLUSION

In this work, we have introduced new functionalities to support privacy in CARiSMA. Moreover, through analyzing a set of given privacy and security requirements, CARiSMA assists a system designer to express security and privacy requirements within models. Specifically, through a pre-analysis of such requirements, a help report is generated, which assists a system designer to annotate a system model with corresponding UML profiles. Furthermore, the pre-analysis automatically generates a CARiSMA analysis according to the given requirements.

We applied CARiSMA to an industrial case study in the context of the VisiOn EU project. The results indicate that CARiSMA successfully supports the analysis of privacy and security requirements in public administration systems. More details on this can be found in the screen cast (https://youtu.be/b5zeHig3ARw).

ACKNOWLEDGEMENTS

This research was partially supported by: (I) Visual Privacy Management in User Centric Open Environments (EU's Horizon 2020 program, No. 653642), (II) Design For Future – Managed Software Evolution (DFG's SPP 1593, project JU 2734/2-2)

REFERENCES

[1] Ahmadian, A. S., Strüber, D., Riediger, V., and Jürjens, J. Model-based Privacy Analysis in Industrial Ecosystems. In *ECMFA* (2017), Springer. accepted.

[2] Barker, K., Askari, M., Banerjee, M., Ghazinour, K., Mackas, B., Majedi, M., Pun, S., and Williams, A. *A Data Privacy Taxonomy.* Springer, 2009, pp. 42–54.

[3] Cavoukian, A., and Chibba, M. Advancing Privacy and Security in Computing, Networking and Systems Innovations through Privacy by Design. In *CASCON* (2009), pp. 358–360.

[4] Colombo, P., and Ferrari, E. Towards a Modeling and Analysis Framework for Privacy-Aware Systems. In *SOCIALCOM-PASSAT* (2012), IEEE Computer Society, pp. 81–90.

[5] Danezis, G., Domingo-Ferrer, J., Hansen, M., Hoepman, J., Métayer, D. L., Tirtea, R., and Schiffner, S. Privacy and data protection by design - from policy to engineering. *CoRR abs/1501.03726* (2015).

[6] den Braber, F., Hogganvik, I., Lund, M. S., Stølen, K., and Vraalsen, F. Model-based security analysis in seven steps — a guided tour to the coras method. *BT Technology Journal 25*, 1 (2007), 101–117.

[7] Georg, G., Ray, I., Anastasakis, K., Bordbar, B., Toahchoodee, M., and Houmb, S. H. An Aspect-oriented Methodology for Designing Secure Applications. *INFSOF 51*, 5 (2009), 846–864.

[8] Gollmann, D. *Computer Security.* John Wiley & Sons, Inc., New York, NY, USA, 1999.

[9] Heitmeyer, C. L., Archer, M., Leonard, E. I., and McLean, J. Applying Formal Methods to a Certifiably Secure Software System. *IEEE Trans. Software Eng. 34*, 1 (2008), 82–98.

[10] Islam, S., Mouratidis, H., and Jürjens, J. A framework to support alignment of secure software engineering with legal regulations. *Software & Systems Modeling 10*, 3 (2011), 369–394.

[11] Islam, S., Pavlidis, M., Mouratidis, H., and Kearney, P. Modeling Trust Relationships for Developing Trustworthy Information Systems. *Int. J. Inf. Syst. Model. Des. 5*, 1 (2014), 25–48.

[12] Jin, X., Sandhu, R., and Krishnan, R. *RABAC: Role-Centric Attribute-Based Access Control.* Springer, 2012, pp. 84–96.

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

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

[15] Katt, B., Gander, M., Breu, R., and Felderer, M. Enhancing Model Driven Security through Pattern Refinement Techniques. In *FMCO* (2011), pp. 169–183.

[16] Lano, K., Clark, D., and Androutsopoulos, K. Safety and Security Analysis of Object-Oriented Models. In *SAFECOMP* (2002), Springer, pp. 82–93.

[17] Lodderstedt, T., Basin, D., and Doser, J. SecureUML: A UML-Based Modeling Language for Model-Driven Security. In *UML* (2002).

[18] Mouratidis, H., Giorgini, P., and Manson, G. Modelling Secure Multiagent Systems. In *AAMAS* (2003).

[19] Nguyen, P. H., Yskout, K., Heyman, T., Klein, J., Scandariato, R., and Traon, Y. L. SoSPa: A System of Security Design Patterns for Systematically Engineering Secure Systems. In *MoDELS* (2015), pp. 246–255.

[20] Object Management Group. Object Constraint Language - Version 2.4. Tech. Rep. formal/2014-02-03, 2014.

[21] Paja, E., Dalpiaz, F., and Giorgini, P. Modelling and reasoning about security requirements in socio-technical systems. *Data and Knowledge Engineering 98* (2015), 123–143. Research on conceptual modeling.

[22] Paja, E., Dalpiaz, F., Poggianella, M., Roberti, P., and Giorgini, P. Sts-tool: Socio-technical security requirements through social commitments. In *2012 20th IEEE International Requirements Engineering Conference (RE)* (Sept 2012), pp. 331–332.

[23] Pavlidis, M., and Islam, S. SecTro: A CASE Tool for Modelling Security in Requirements Engineering using Secure Tropos. In *CAiSE* (2011), pp. 89–96.

[24] Peldszus, S., Kulcsár, G., Lochau, M., and Schulze, S. Continuous detection of design flaws in evolving object-oriented programs using incremental multi-pattern matching. In *Proceedings of the 31st IEEE/ACM International Conference on Automated Software Engineering* (New York, NY, USA, 2016), ASE 2016, ACM, pp. 578–589.

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

[26] Schneider, K., Knauss, E., Houmb, S., Islam, S., and Jürjens, J. Enhancing Security Requirements Engineering by Organisational Learning. *REJ 17*, 1 (2012), 35–56.

[27] Spiekermann, S., Acquisti, A., Böhme, R., and Hui, K.-L. The challenges of personal data markets and privacy. *Electronic Markets 25*, 2 (2015), 161–167.

[28] Spiekermann, S., and Cranor, L. F. Engineering Privacy. *IEEE Trans. Softw. Eng. 35*, 1 (Jan. 2009), 67–82.

[29] Steinberg, D., Budinsky, F., Paternostro, M., and Merks, E. *EMF: Eclipse Modeling Framework 2.0*, 2nd ed. Addison-Wesley Professional, 2009.

[30] The European Parliament and the Council of the Europeam Union. 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* (2016).