Access Control Policy Administration supporting User-defined Privacy Preferences
A Use-case in the context of Patient-centric Health-care

Thomas Trojer and Ruth Breu (Supervisor)

Institute of Computer Science, University of Innsbruck, Austria
thomas.trojer@uibk.ac.at

Abstract. The protection of medical records is understood to be an issue related to privacy and therefore closely bound to the patient her-/himself, playing a crucial role in networked electronic health-care. Awarding users to have control over personal data stored and processed by information systems is important as it allows a user to communicate individual privacy concerns. Still, users self-maintaining controls of access to their personal data poses challenges regarding its implementation. A major issue is that users are typically non-security experts and have only limited knowledge of the context domain. Regarding our use-case patients may not be fully familiar with all activities related to information processing e.g., during a medical treatment, therefore not able to properly decide on privacy and authorization measures. In our work we discuss the development of access control authoring tools to allow non-expert users to create, analyse and adjust personal privacy policies. We propose the integration of domain aspects into the development process of such tools. With extended knowledge about the domain the creation of policy rules can be bound to high-level activity descriptions and policy analysis can be performed in a domain-aware manner.

1 Motivation

Modern information systems are able to store, retrieve an process vast amounts of data. Further extended by networking capabilities and driven by the increased personal use of information technology a wide range of data can be collected and combined to form new processable content. The collection of data can be critical without means of regulating access to it when requests for provisioning or processing are made. With respect to the actual use-case, data can be considered as e.g., confidential according to its content or sensitive in terms of identifying individual persons.

In a common use-case scenario a person responsible for security matters, like an administrator, defines access control policies which constitute appropriate security measures for all protected resources. In the case of person-identifying information, such policies do not necessarily reflect the conception of the identified individual on how to access-protect these information. By declaring privacy as a right about *information self-determination*, e.g., within the *European Data*

Protection Directive[1] an individual user is awarded a distinguished role within privacy management processes. This can be interpreted as the required ability of a user to influence the definition of enforceable access control policies which constitute data privacy related to the user's personal conception.

1.1 Use-case: Patient-centric Electronic Health-care

We consider a use-case from the Austrian e-Health initiative which started in 2006 as a governmental workgroup. A central goal of this initiative is the establishment of a distributed shared electronic health-record for all citizens of Austria. It has been shown that a holistic medical history of a patient improves the health-care infrastructure from an economical perspective as well as from a viewpoint of effectiveness regarding medical treatments. Still, because of the high degree of sensitivity which is observed in most medical data, privacy is a concern of utmost importance to be tackled. In the context of this initiative we want to contribute methods with a strong focus on patient-centricity by establishing personal control over privacy-relevant health data.

2 Problem statement

A general problem question can be raised as follows: *How can a user, considered a non-security and non-domain expert, be supported during the declaration of access control policies in a way that she/he is aware about consequences to certain evaluation criteria, first and foremost personal privacy and e.g., the effectiveness of the information system.* Two potential user actions can be derived from this problem question. First, a user has to be provided with tools to create access control policies and second a currently active policy has to be visualized in a way that the user can understand how it influences the information flow of the system. Visualizing active policies is especially important to allow a user to reconsider the policies' appropriateness. Therefore a user is able to adjust a policy in a way so that it fits her/his personal conception of access control.

3 Contributions

We contribute a framework using domain characteristics to develop user interfaces for access control policy authoring. Further this framework includes a policy analysis component capable of providing users with feedback during their actions within the policy authoring process. A central step to be performed is therefore the modeling of domain entities and their relationships as well as the annotation of the domain model with attributes from the access control domain. In the context of our use-case we identify e.g., a *medical practitioner* or *pharmacist* as *subjects* of access control, whereas *medical records* or *referrals* are considered

[1] see Directive 95/46/EC, `http://ec.europa.eu/justice/policies/privacy/law/index_en.htm`

resources to be protected by access control. A basic API to work with domain entities and access control policy elements can be generated from that model.

Based on this model we designed a generic authoring process [10] that leads to the creation of access control policies. This process allows for policy creation and adaptation, which can be triggered by the user.

In this work we want to emphasize two research directions in order to reach our objective of providing a non-expert user with access control authoring tools to establish privacy policies. These are described in the following sections.

3.1 Scenario-based Access Control Policy Authoring

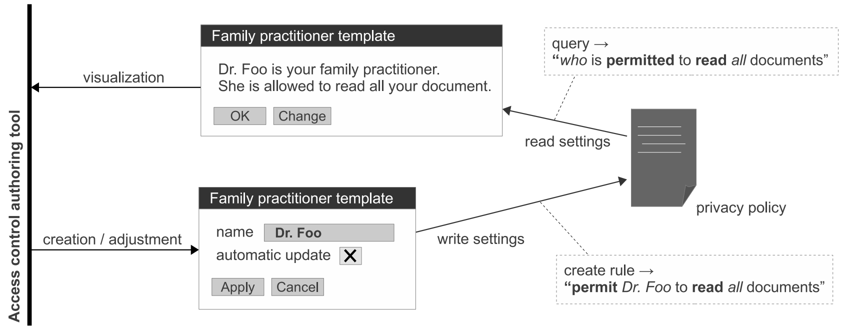
John Carroll [3] coined the term *scenarios* as stories about people and their activities, e.g., related to the tasks of their work. We propose *scenario-based authoring* as a method to create and further visualize access control policies in a usable way. This is important as users typically lack of knowledge about the underlying access control concepts and therefore have to be supported during the authoring process [12, 2].

The first step of our approach regards the elicitation of typical working activities of the domain. Only working activities which involve information processing in an arbitrary way are considered as they can be related to access control. In our context we tackled this step by performing a case-study about stakeholders and some of their activities in the domain of electronic health records in Austria [9]. Next the selected working activities have to be translated to our template language. A template consists of the attributes identifying and describing the working activity in natural language and further a set of access control rules which are written to the user policy once a template instance is executed. User control is established via user interface form input fields which represent domain and environment information (e.g. time, date, location or cardinalities) and are bound to variables used within the policy rules of the template. Fig. 1 shows a basic scenario from our electronic health-care use-case, namely, the selection of a family practitioner performed by a citizen stakeholder. In this example two inputs are provided, the name of the family practitioner and whether all documents (i.e. also all future ones) shall be accessible or only the ones currently stored about a patient. By executing a template instance one permit-rule is created allowing the selected practitioner (i.e. the subject of the access control target) to access patient health records. Similarly a query can be formed to visualize a selected family practitioner to the user by asking who is permitted to read all documents.

The template language including access control rules and queries are currently developed and described in a formal way. With this work we target the field of usable security.

3.2 Domain-based Access Control Policy Analysis

We see two situations where a user may be encouraged to reconsider her/his access control settings and to adjust them if necessary. First, if the representation



Family practitioner template

Dr. Foo is your family practitioner.
She is allowed to read all your document.

Family practitioner template

name: Dr. Foo
automatic update ☒

query → "*who* is **permitted** to **read** *all* documents"

create rule → "**permit** *Dr. Foo* to **read** *all* documents"

Fig. 1. Scenario-based policy authoring leading to privacy policies and visualization.

of currently active settings can be provided in a readable way the user is able to detect differences between these settings and her/his intended settings. Therefore we propose to use scenario-based policy templates (see Section 3.1) to increase understandability of a user policy.

Besides a user adjusting her/his policy based on a manual interpretation, policies may also carry conflicts or influence arbitrary system properties and the user in a negative way. Therefore we identify a second situation for adjusting a policy, namely triggered by feedback of a performed policy analysis. In general policy analysis is extensively discussed in literature (see e.g., [7, 8, 1]), but mainly based on conflict detection regarding the interplay of different policy rules. Work, as e.g., done by Michael LeMay [6] and Katie Fisler [4] consider a policy model together with the domain where policies are deployed on. Based on these works we propose the definition of high-level evaluation criteria which interact. These criteria can be attached to the policy authoring activity leading to a balancing act during access control configuration in order to satisfy best all evaluation criteria. In our previous work [9] we considered *privacy* and *information system effectiveness* as evaluation criteria to be balanced. There, based on a domain model and models for each evaluation criteria, domain-aware analysis rules integrating all evaluation aspects can be generated.

For our use-case we defined a trivial privacy model consisting of permissions and restrictions and an information system effectiveness model. This effectiveness model consists of personal relationships between subjects and needs-to-know relations between subjects and protected resources (see Fig. 2). Regarding privacy the lack of a permission can be interpreted as increased privacy. On the other hand the absence of one or both the personal relationship or the needs-to-know relation decreases the need of the information system to be effective towards these attributes. E.g. a family practitioner earns an associated personal relationship connecting her/him to the patient, further needs-to-know relations to all patient's data are established. Now, a patient restricting this practitioner from reading any data would obviously contribute to the her/his privacy, still the health-care information system would not effectively operate anymore. An effectiveness warning with detailed information about its reasons is provided to the user, which in turn may react on it by adjusting her/his settings.

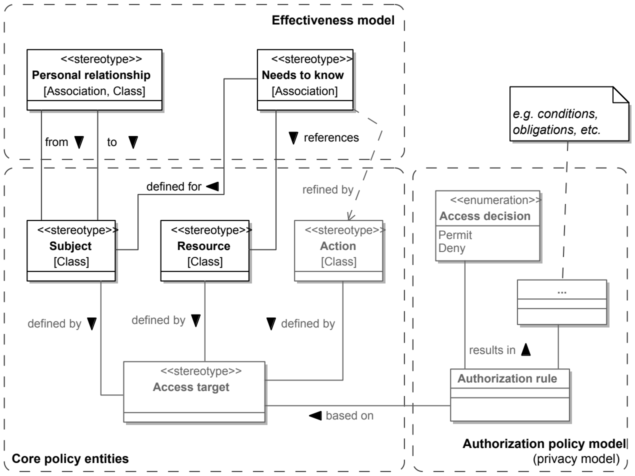


Fig. 2. Evaluation criteria *privay* and *effectiveness* applied to core policy entities and used for domain-aware policy analysis.

4 Research Plan

In an ongoing project with our industry partner *ITH-icoserve for healthcare technology*, a subsidiary company of Siemens and a local hospital provider, we are developing an access control policy authoring application based on a secured IHE-based infrastructure [2] for shared patient health-records.

Currently we have considered access control enforcement based on IHE XDS[2] and auxiliary profiles [5, 10], for which our industry partner is an implementer and tested for conformity and interoperability. Further a prototypical authoring portal application was developed [9]. In order to let the policy authoring reflect the actual domain, we employ a model-driven process which generates a policy API based on a domain and access control model [11]. Our approach for domain-aware policy analysis, which is based on balancing of evaluation criteria will also build upon the policy API. Evaluation criteria we currently consider is the correlation between permitted or restricted access, personal relationships between stakeholders and the importance to have certain data available to specific stakeholders. In future work we also want to study other criteria, e.g., the purpose-relatedness of permitted data accesses.

[2] see IHE IT-Infrastructure Technical Framework, `http://www.ihe.net/Technical_Framework/index.cfm#IT`

Generally we apply methods from design science to develop the aforementioned artifacts for patient-controlled access control. Usable methods for authoring and analysis of policies are our main focus. Further we will perform additional case studies to justify the application of these approaches within our use-case. As human interaction with the authoring application is a central part of this work, therefore we will also conduct a usability study to evaluate the usefulness of working scenarios and templates to maintain access control policies. A fully features authoring portal application is planned to be integrated into a health information system built by our industry partner and deployed to our regional health-care infrastructure. This will consist of templates for adapting authorization policies as well as policy analysis to inform a citizen about the consequences of certain access control settings. Finally the deployed system has to be evaluated regarding its performance and user acceptance.

References

1. E. Bertino, B. Catania, E. Ferrari, and P. Perlasca. A logical framework for reasoning about access control models. In *Proceedings of the sixth ACM symposium on Access control models and technologies*, SACMAT '01, 2001.
2. S. Brostoff, M. A. Sasse, D. Chadwick, J. Cunningham, U. Mbanaso, and S. Otenko. R-What? Development of a Role-Based Access Control (RBAC) Policy-Writing Tool for e-Scientists. *Software: Practice and Experience*, 35(9):835–856, July 2005.
3. J. Carroll. Five reasons for scenario-based design. *Interacting with Computers*, 13(1):43 – 60, 2000.
4. K. Fisler and S. Krishnamurthi. A model of triangulating environments for policy authoring. In *Proceeding of the 15th ACM symposium on Access control models and technologies*, SACMAT '10, 2010.
5. B. Katt, T. Trojer, R. Breu, T. Schabetsberger, and F. Wozak. Meeting ehr security requirements: Seaas approach. In *EFMI STC 2010. Accepted*, June 2010.
6. M. LeMay, O. Fatemieh, and C. A. Gunter. PolicyMorph: interactive policy transformations for a logical attribute-based access control framework. In *Proceedings of the 12th ACM symposium on Access control models and technologies*, SACMAT '07, 2007.
7. E. Lupu and M. Sloman. Conflicts in Policy-based Distributed Systems Management. *IEEE Transactions on Software Engineering*, 25, 1999.
8. J. D. Moffett and M. S. Sloman. Policy conflict analysis in distributed system management, 1993.
9. T. Trojer, B. Katt, T. Schabetsberger, R. Breu, and R. Mair. Considering privacy and effectiveness of authorization policies for shared electronic health records. In *ACM IHI 2012 (in press)*, 2012.
10. T. Trojer, B. Katt, T. Schabetsberger, R. Mair, and R. Breu. The Process of Policy Authoring of Patient-controlled Privacy Preferences. In *eHealth 2011*.
11. T. Trojer, B. Katt, F. Wozak, and T. Schabetsberger. An Authoring Framework for Security Policies: A Use-case within the Healthcare Domain. In *eHealth 2010*, 2010.
12. T. Whalen, D. Smetters, and E. F. Churchill. User experiences with sharing and access control. In *CHI '06 extended abstracts on Human factors in computing systems*, CHI EA '06, pages 1517–1522, New York, NY, USA, 2006. ACM.