The Process of Policy Authoring of Patient-Controlled Privacy Preferences*

Thomas Trojer[1], Basel Katt[1], Thomas Schabetsberger[2],
Richard Mair[2], and Ruth Breu[1]

[1] Research Group Quality Engineering, University of Innsbruck, Austria
{thomas.trojer,basel.katt,ruth.breu}@uibk.ac.at
[2] ITH-icoserve GmbH, Innsbruck, Austria
{thomas.schabetsberger,richard.mair}@ith-icoserve.com

Abstract. Discussions about appropriate security controls to protect medical records led to the understanding that the patient her-/himself plays a crucial role in networked electronic health-care. Patients have individual privacy concerns and may want to execute their personal right of self-determination on access and usage of their medical records. The ability for patients to have control over their personal medical data is the essence of patient-centric networked electronic health-care, but poses challenges regarding its tool support. Since patients can be generally treated as non-security experts as well as non-health-care domain experts, usability-supporting factors of authoring tools for privacy preferences have to receive major attention by implementers. Additionally, domain characteristics have to influence the design of such authoring applications. Finally expressed privacy preferences have to be analysed to inform the patient-author and guide her/him in the policy authoring process. In this paper we discuss the process of authorization policy authoring for shared electronic health records which we use to implement patient-controlled access control authoring tools. Further a use-case in the context of a specific health-care infrastructure is presented.

Keywords: Privacy, Patient privacy policy, Access control, Authoring tools, Information self-determination, Integrating the Healthcare Enterprises (IHE).

1 Introduction

Discussions (e.g., in [9]) about appropriate security controls to protect personal medical records led to the understanding that the patient her-/himself plays a crucial role in networked electronic health-care. This is due to the fact that a patient constitutes the identified individual within a health-record and therefore processing of such medical data is bound to common data privacy regulations of

* This work was partially supported by the Austrian Federal Ministry of Economy as part of the Laura-Bassi – Living Models for Open Systems – project FFG 822740/QE LaB, see http://lab.q-e.at/

P. Kostkova, M. Szomszor, and D. Fowler (Eds.): eHealth 2011, LNICST 91, pp. 97–104, 2012.

a country (see e.g., [1]). Further patients have individual privacy concerns and may want to execute their personal right of self-determination on access and usage of their medical records. Legal regulations on data privacy and therein especially information self-determination represent the underpinning motive to let patients express personal privacy concerns. To meet these regulations, customized applications and IT-infrastructure have to be built to make electronic health-records controllable.

Therein we see a major requirement being usable authoring tools supporting and guiding patient-authors of privacy preferences during the authoring process. An important usability-supporting factor during this authoring process is the analysis of privacy policies. Analysis results are used to inform the patient-author about quality and effects her/his privacy settings imply on the overall functionality of the health-care information system. Besides policy analysis, the integration of health-care domain characteristics and domain knowledge also support usability. Such integrations try to answer questions like, *"who are the typical stakeholders within the health-care domain?"*, *"which data is involved and how sensitive is it?"* or *"what data is required by those stakeholders?"*. In this paper we present the process of authorization policy authoring for shared electronic health records and discuss usability-supporting factors involved. The importance of developing highly usable authoring tools comes from the fact that patients are not considered security experts and are not necessarily familiar with working processes of the health-care domain. Therefore patients have to be supported when trying to express their individual conception of privacy towards corresponding enforceable privacy policies.

2 Problem Statement

Privacy can be ensured when a consent or agreement on a purpose of use is stated by the identified individual which gets enforced by the security infrastructure. Further access restrictions limit usage of data in order to prevent potential damage and misuse. Here we want to specifically emphasize on the necessity that the explicit source for setting privacy preferences is the corresponding patient.

A problem gets visible when changing the perspective, asking how privacy policies can be declared in a way so that they match patients' individual conception of privacy. Since it is not feasible to put in place a trusted party who manages policies for each patient, a patient by her-/himself should be allowed to act as the author of privacy settings. An initial requirement to successfully empower patients to do so, is to consider usability-supporting factors of the policy authoring tools. These factors leads to a change in the traditional authoring process, which allows only security experts to define security artifacts. Furthermore, as privacy policy authoring requires health-care domain information, aspects of integration to an established health-care infrastructure have to be covered at the same time.

3 Related Work

Our ongoing work related to patient-controlled access control is based on proposals published by ELGA[1], which is the working group driving the Austrian e-health initiative [2].

There has been general work published in the field of usable security, e.g., [7]. The authors in this work state that when employing usable applications, guiding the user in a privacy policy authoring process will lower the risk of inappropriate use of personal information. In their work they conducted an empirical study to evaluate the use of tools guiding and not guiding users through the authoring process. Significant advantages of the employment of guided tools are shown in their study. This also justifies our effort on implementing patient-controlled access control policy authoring. Still, our work differs by the use-case within the health-care domain together with the domain-aware analysis of patient privacy policies to support the user. Further the authors in [13] evaluated the SPARKLE policy workbench, an enterprise privacy policy authoring application in order to gain information on usability challenges. We are able to develop our usability requirements based on parts of their work, although related to characteristics of a networked health-care landscape.

A core part of the process of policy authoring we propose in this work is authorization policy analysis. An analysis component therefore analyses patient privacy settings and provides feedback to the patient-author. Policy analysis, similar to what we implemented is covered in [10]. Still, in our work we dynamically retrieve health-care domain characteristics, required to enable domain-aware analysis.

Katt et al. [8] propose an architecture for enforcing access control in *Integrating the Healthcare Enterprises* (IHE) based systems. IHE is also the basis for our work regarding the retrieval of domain characteristics. Their work can be used to implement the actual enforcement of patient privacy policies.

4 Authoring of Privacy Preferences

In this section we define the authoring process and discuss usability-supporting factors of authoring of privacy preferences performed by non-security experts. In order to allow those privacy preferences to be machine-interpretable and enforceable by a security infrastructure we translate them to access control policies.

Fig. 1 describes the activities and artifacts involved in our policy authoring process. Based on the type or expertise of a user, a set of templates for declaring privacy settings is gathered and made accessible to the user. After setting privacy options based on domain information a policy analysis component decides whether the privacy policy is enforceable or needs to undergo further editing. From this process we extract factors which play a part in supporting the usability of policy authoring tools. These usability-supporting factors are shown in

[1] electronic health-record (German, "Elektronische Gesundheitsakte")

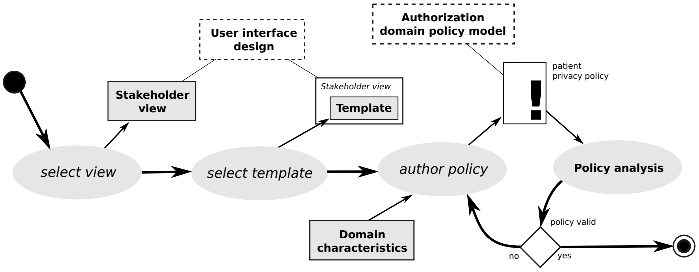

Fig. 1. Authorization policy authoring process represented as activity diagram

Fig. 2 as part of our authorization policy authoring framework. A central building block of this framework is the *authorization policy authoring model* which provides entities required to be presented by *policy authoring user interfaces* as well as to be translated into *patient privacy policies*. Entities of this model correspond to the health-care domain and define authorization aspects. These authorization aspects are introduced to the model via extending the *authorization domain policy model* (cf. our previous work [14]). The authorization domain policy model defines e.g., an *access target* describing the requesting *subject* and an *action* to be executed on an information system *resource*. Further *permission* or *restriction* entities cover those access targets and further limit access by additionally providing *conditions* or *obligations* to be fulfilled. Based on these definitions enforceable access control policies can be generated. Fig. 2 indicates this via the vertical connections between the policy authoring user interfaces and the patient privacy policy through the authorization policy authoring model.

Below we discuss the usability-supporting factors related to authorization policy authoring. *User interface design* and *stakeholder views* are only conceptionally mentioned here, since the actual design of authoring tools as well as studies on user groups and detailed use-case scenario analysis, respectively, are out of scope and considered future work.

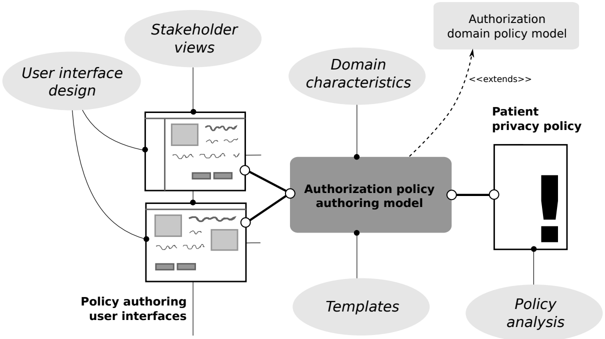

Fig. 2. Usability-supporting factors of access control policy authoring

Stakeholder Views. A stakeholder view defines the authoring functionality which is available for a specific type of user, e.g., a patient or medical professional. By analysing different use-case scenarios, where access to a shared electronic health record of a patient is involved, all required stakeholder views can be identified. A typical use-case scenario regarding a patient is the viewing of her/his own health record or the definition of trusted medical staff gaining extended access rights to health records. On the other hand, medical practitioners want to access the health record of a patient during or after a medical treatment or want to have the option to protect very critical health records from patient access (e.g. if laboratory markers suggest to diagnose a severe disease).

Having different views allows us to define multiple customized applications related to one authorization policy authoring model, expressing the needs of different stakeholders. Further, when developing views according to this model, we can guarantee that the user interface reflects domain and access control aspects appropriately.

User Interface (UI) Design. When defining graphical user interfaces human cognition as well as user behavior during task execution has to be considered. A usable UI is designed in a way e.g., to show interface elements in a well-placed (grouped) manner, describes necessary steps to reach a certain goal, gives a user a history of previous actions taken, lets a user abort (and maybe continue) at any time and keeps a user informed about the application state. In our case the state of the application links back to *policy analysis* as it will be described later in this section.

Domain Characteristics. Policies employed by a security infrastructure may be diverse and complex. A patient's ability to define privacy policies may be influenced by multiple information sources from within the electronic health-care network. Auxiliary information have to be used by the policy authoring application in order to enable a domain-aware policy authoring process. We identify the following types of domain-related information and associated attributes to be integrated:

- *Patient*, i.e. unique patient identifiers, corresponding health records, related medical practitioners, etc.
- *Medical data*, i.e. record identifiers, record types, related stakeholders (e.g., creator or identified patient)
- *Health-care provider*, i.e. working roles, unique identifiers
- *Health-care work processes*, i.e. record type – working role mappings, types and purposes of data processing, patient – practitioner relationships (via medical treatments, referrals or maintained health records), practitioner – resource *needs-to-know* [4] relationships, etc.

Domain characteristics represent the core factor to actually implement usable policy authoring tools. Integration of domain characteristics in the context of an IHE-based health-care infrastructure is discussed in Section 5.

Templates. Templates are partial instances of the authorization domain policy model. A template covers a common concept of a health-care working environment which implies an authorization rule supporting it. Templates are defined via a *label* which associates entities of the authorization domain policy model (used as placeholders) and the actual domain data specified by domain characteristics. The total amount of available templates defines the instantiation possibilities of the underlying authorization domain policy model. Therefore templates have to be based on evaluated use-case scenarios in order to be meaningful and to provide guidance and an overview of functionality to the user. Finally for each template different *stakeholder views* and *user-interface* designs can be considered.

E.g., the template with the label *family practitioner* associates an authorization domain policy stating that the *selected medical practitioner* (i.e. a placeholder for domain data) is *permitted* (i.e. an instance of the *permission* entity) to access *all health records* (i.e. the actual domain data of type health record). As another example, a template labeled *referral* associates a policy which allows a *selected medical practitioner* (i.e. the target of the referral) to access (i.e. a stated *permission*) a basic set of health records (e.g., defined via *record types* or via the (derived) *record sensitivity*) of a *patient.* Such templates, as they correspond to the describing authorization domain policy model can be easily transformed to enforceable access control policies, e.g., expressed by the *Extensible Access Control Markup Language* (XACML) [12].

Policy Analysis. Policy analysis is in general considered a recurring task. By analyzing policy artifacts, feedback can be provided to inexperienced or non-expert users. In our context, a patient expressing privacy preferences can be informed e.g., if certain access rules are in conflict. Further a patient has to be warned if her/his settings would lead to privacy at risk or interfere with working processes in the health-care domain, e.g., by restricting access to medical data where access is required.

By assuming syntactically valid authorization policies, we see two different types of analysis to be performed:

- *Conflict* or *redundancy detection* between policies (see e.g., [11]), i.e. access control is undecidable or one policy dominates another policy, respectively
- *Constraint checking* regarding health-care work processes, i.e. evaluating if e.g., privacy is potentially at risk as no inter-personal relationship between a patient and a practitioner can be derived

Policy analysis is bridging the gap between patients and security and domain experts. On one side patients request privacy protection which conforms to their conception of privacy and on the other side security experts are able to actually express such preferences in a machine-readable way. Further domain experts can contribute knowledge about properties for a functioning health-care domain. A policy analysis component functions herein as a kind of advisory system to a patient. By reporting issues regarding domain characteristics together with the authorization policies themselves, policy analysis positively contributes to the usability of an authoring application.

5 Use-Case: Authoring Tools for IHE IT Infrastructure

In order to establish authorization policy authoring tools in the context of a health-care network infrastructure, we have to identify the required interfaces for retrieving domain characteristics and build upon a specific access control framework. The Austrian ELGA proposes the use of IHE-based systems together with authorization enforcement via an XACML infrastructure. Fig. 3 shows the IHE-profiles which the authoring applicaton integrates, as well as XACML security components it relates to. Detailed descriptions of the security components, their interaction and access control mechanisms are found in [8,12,6] and out of scope of this specific work.

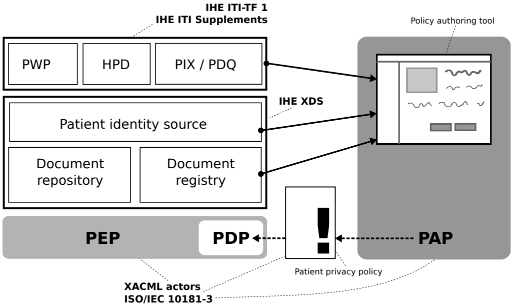

Fig. 3. Integration of policy authoring tools, their relation to the XACML actors and their dependencies to an IHE-based infrastructure

In the following we identify and list different IHE-profiles the authoring application needs to incorporate:

- *Cross-enterprise document sharing* (XDS) [3] *document registry*, in order to support retrieval of *medical data* and *health-care work processes* domain characteristics (cf. Section 4 – *Domain characteristics*)
- XDS *patient identity source*, in order to get local patient information (e.g., from within a specific hospital) as part of the *patient* domain characteristics
- *Patient identifier cross-referencing* (PIX) and *patient data query* (PDQ) [3], to support a unified patient identifier and the retrieval of extensional patient information as part of *patient* domain characteristics, respectively
- *Healthcare provider directory* (HPD) [5] to fetch provider meta-data like work role or credentials, as part of *health-care provider* domain characteristics
- *Personnel white pages* (PWP) [3], to gain extensional provider information as part of *health-care provider* domain characteristics

Employing these profiles within a health-care network maintaining electronic health records enables highly domain-aware policy authoring. The Austrian ELGA and our business partner *ITH-icoserve* correspond to IHE profiles, allowing our work to be put in a practical context.

6 Conclusion and Future Work

In this paper we described usability-supporting factors for developing effective authorization policy authoring tools. The authoring application enables patient-controlled privacy preferences which get transformed to enforceable access control policies. These policies protect access to shared medical data within a networked electronic health-care system. We elucidated factors related to the design of such application which are related to the authorization policy model, domain characteristics influencing the specification of policies and the analysis of policies to provide feedback to the patient-author of policies. Finally we described a use-case of an IHE-based health-care infrastructure and a set of IHE profiles to be integrated within an authorization policy authoring tool. These profiles define the required interfaces to retrieve domain characteristics.

Future work discusses three major work packages: (i) Usability studies guiding the design of user-interfaces and stakeholder views, (ii) a more formal discussion of policy analysis regarding policy conflicts and domain-related constraints and (iii) experiences from our efforts on integrating our authoring prototype to the national health-care network in conformance to all national regulations.

References

1. European Commision. Directive 95/46/EC, Data Protection Directive (1995)
2. IBM Austria. Feasibility Study for implementing the electronic health record (ELGA) in the Austrian health system (2006)
3. IHE. IT Infrastructure (ITI) Technical Framework. Integration Profiles, vol. 1
4. IHE. IT Infrastructure Access Control (White Paper) (2009)
5. IHE. IT Infrastructure (ITI) Technical Framework, Supplement, Healthcare provider directory (HPD) (2010)
6. ISO. ISO/IEC 10181-3:1996 Information technology – Open Systems Interconnection – Security frameworks for open systems: Access control framework (1996)
7. Karat, C., Karat, J., Brodie, C., Feng, J.: Evaluating interfaces for privacy policy rule authoring. In: CHI 2006. ACM (2006)
8. Katt, B., Breu, R., Hafner, M., Schabetsberger, T., Mair, R., Wozak, F.: Privacy and Access Control for IHE-Based Systems. In: Weerasinghe, D. (ed.) eHealth 2008. LNCSIT, vol. 1, pp. 145–153. Springer, Heidelberg (2009)
9. Kotschy, W.: STRING ELGA Datenschutzrechtliche Analyse (German, Electronic health record – Data privacy aspects). Austrian Federal Ministry of Health (2005)
10. LeMay, M., Fatemieh, O., Gunter, C.A.: PolicyMorph: Interactive Policy Transformations for a Logical Attribute-Based Access Control Framework. In: SACMAT 2007. ACM (2007)
11. Moffett, J.D., Sloman, M.S.: Policy conflict analysis in distributed system management (1993)
12. OASIS. eXtensible Access Control Markup Language (XACML) v2.0 (2005)
13. Reeder, R.W., Karat, C.-M., Karat, J., Brodie, C.: Usability Challenges in Security and Privacy Policy-Authoring Interfaces. In: Baranauskas, C., Abascal, J., Barbosa, S.D.J. (eds.) INTERACT 2007. LNCS, vol. 4663, pp. 141–155. Springer, Heidelberg (2007)
14. Trojer, T., Katt, B., Wozak, F., Schabetsberger, T.: An Authoring Framework for Security Policies: A Use-Case within the Healthcare Domain. In: Szomszor, M., Kostkova, P. (eds.) e-Health. LNICT, vol. 69, pp. 1–9. Springer, Heidelberg (2011)