Managing Privacy and Effectiveness of Patient-Administered Authorization Policies

Thomas Trojer, University of Innsbruck, Austria
Basel Katt, University of Innsbruck, Austria
Ruth Breu, University of Innsbruck, Austria
Thomas Schabetsberger, ITH-icoserve Technology for Healthcare, Austria
Richard Mair, ITH-icoserve Technology for Healthcare, Austria

ABSTRACT

A central building block of data privacy is the individual right of information self-determination. Following from that when dealing with shared electronic health records (SEHR), citizens, as the identified individuals of such records, have to be enabled to decide what medical data can be used in which way by medical professionals. In this context individual preferences of privacy have to be reflected by authorization policies to control access to personal health data. There are two potential challenges when enabling patient-controlled access control policy authoring: First, an ordinary citizen neither can be considered a security expert, nor does she or he have the expertise to fully understand typical activities and workflows within the health-care domain. Thus, a citizen is not necessarily aware of implications her or his access control settings have with regards to the protection of personal health data. Both privacy of citizen’s health-data and the overall effectiveness of a health-care information system are at risk if inadequate access control settings are in place. This paper refers to scenarios of a case study previously conducted and shows how privacy and information system effectiveness can be defined and evaluated in the context of SEHR. The paper describes an access control policy analysis method which evaluates a patient-administered access control policy by considering the mentioned evaluation criteria.

Keywords: Access Control Policies, Conflict Resolution, Information System Effectiveness, Policy Analysis, Privacy, Shared Electronic Health Records (SEHR)

INTRODUCTION

Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others (Westin, 1967). Therefore data privacy defines itself as a protection mechanism to mitigate personal damage when data can be brought into the context of individual persons. A central build-
ing block of privacy is the individual right to decide which data about oneself might be collected and stored and how data is supposed to be processed (OECD, 1980). Since 1983 this right, entitled informational self-determination is a fundamental right in German law¹ (law of the German federal constitution (BVerfGE) 65, 1) and further is a substantial part of the European Data Protection Directive 95/46/EC (European Commission, 1995) established all over the European Union (EU) through corresponding national laws.

Despite the right of individual users to participate in activities to control privacy-sensitive information, its implementation is difficult and poses at least the following challenges: An ordinary user is typically not considered a security expert and the actual definition or selection of appropriate authorization preferences requires the user to translate her/his mental conception of privacy into enforceable security configurations. Another issue comes with the impact user-defined settings of authorization may have to the user’s privacy or the resulting effectiveness of the health-care information system. Users, as the sole authors of access control statements, have to be made aware about the consequences there settings imply. Although issues regarding the authoring of access control settings have been well discussed in literature, e.g., by suggesting usable authoring tools, like the line of work done by Karat, Karat, Brodie, and Feng (2006) and Reeder, Karat, Karat, and Brodie (2007) proposes, little attention has been paid to the analysis of impact of access control policies to a specific type of information system. In this work we discuss the interrelationship between two specific criteria which can be used to evaluate access control settings enforced by a health-care information system. Further we derive resolution strategies which are proposed to a citizen to support her/him with resolving inadequate security.

Domain Evaluation Criteria

In order to support the management and protection of sensitive health-records, citizens have to be supported by usable policy authoring tools. Such authoring tools should provide means to allow a user to encode her/his privacy concerns into enforceable security configurations. Besides the importance of having such tools being user-friendly, they have to ensure that policies have no negative impact on the system or the user. Depending on the domain, several evaluation criteria may be important to validate the outcomes of access control policy management activities.

We see the interrelation between privacy and information system effectiveness factors as especially important when managing shared electronic health-records and therefore define them as evaluation criteria in this context. Evaluation of privacy criteria have to support the user in matching her/his personal conception of privacy with the preferences currently enforced through corresponding policies. If awareness about the promoted privacy of those policies towards the user can be established, she/he is encouraged to reconsider and adapt access control preferences in case it is required. On the other hand, if the evaluation suggests no issues with the user policy, she/he can be assured about the appropriateness of the enforced privacy settings.

The use of electronic health-records is originally motivated by lowering the costs of medical treatments or medical research as well as to increase the overall effectiveness of the healthcare enterprises. Effectiveness is increased as healthcare information systems can store and provide a holistic and long-term view of a patient’s health status, which can be used e.g., to support a practitioner during a treatment session. As different stakeholders in the medical domain require access to these
BDD-Based Synthesis of Reversible Logic
www.igi-global.com/chapter/bdd-based-synthesis-reversible-logic/63820?camid=4v1a