Chapter 15

Integrating Patient Consent in e-Health Access Control

Kim Wuyts
Katholieke Universiteit Leuven, Belgium

Riccardo Scandariato
Katholieke Universiteit Leuven, Belgium

Griet Verhenneman
Katholieke Universiteit Leuven, Belgium

Wouter Joosen
Katholieke Universiteit Leuven, Belgium

ABSTRACT

Many initiatives exist that integrate e-health systems on a large scale. One of the main technical challenges is access control, although several frameworks and solutions, like XACML, are becoming standard practice. Data is no longer shared within one affinity domain but becomes ubiquitous, which results in a loss of control. As patients will be less willing to participate without additional control strategies, patient consents are introduced that allow the patients to determine precise access rules on their medical data. This paper explores the consequences of integrating consent in e-health access control. First, consent requirements are examined, after which an architecture is proposed which incorporates patient consent in the access control service of an e-health system. To validate the proposed concepts, a proof-of-concept implementation is built and evaluated.

INTRODUCTION

To date, medical data are shared with a single affinity domain (e.g. hospital, group practice, etc.). Because medical information is very sensitive, its controlled access represents a key security requirement. This is also reflected by several legislations like the US Health Insurance Portability and Accountability Act and the EU Data Protection Directive. In this respect several frameworks and solutions, like XACML (Moses, 2005), are already standard practice.

DOI: 10.4018/978-1-4666-2482-5.ch015

Copyright © 2013, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

Currently, many initiatives have emerged that aim toward integrating e-health systems on a larger scale. Well-known examples are the Integrating the Healthcare Enterprise consortium (IHE), the UK National Health System, and the European epSOS project. These initiatives aim at creating a unified Electronic Health Record (EHR) containing patient data provided by a wide range of health-care professionals. As scale increases, e.g. when regional or national e-health systems will be fully operational, data will no longer be contained in a single affinity domain and it will become harder for patients to stay in control of how data is used. This results in concerns for the patient who will be less eager to participate in a ubiquitous e-health system.

Moreover, projects like Google Health and Microsoft HealthVault have successfully introduced the idea of the Personal Health Record (PHR) that is a medical file containing health data provided by the patients themselves. Patients are also more and more engaged with online communities (e.g., PatientsLikeMe) where they can provide and share personal health information with peers. We are at the verge of a deeper and tighter integration among different systems (large scale EHR, PHR, communities), which demands for greater and greater control from the user perspective. Once more, it is simply no longer realistic to expect the patient to outsource the control over her own data to care providers (like hospitals) and service provider (like Google) altogether, especially in a converged environment where many stakeholders are involved.

To counter these concerns, electronic patient consents bear the promise of enabling a user-centric access to own medical data and hence re-establish the trust of the patients. Patient consents are user-defined (often complex) rules providing directives on how access to own data should be regulated. Although this is a crucial part of e-health access control systems (as required by compliance to laws and regulations), the related work is rather limited. Furthermore, the literature is even more inadequate for what concerns the integration of user directives (like patient consents) into the standard practice access control.

As its main contribution, this paper explores the options for representing patient consents and incorporating their directives into the access control decision process. The legal requirements concerning patient consent (with focus on European legislation) are presented first. On top of the results of the legal analysis, we propose a format for representing patient consents and outline the lifecycle governing them, e.g., with respect to their creation and revocation. Finally, we suggest both a policy evaluation algorithm and a reference authorization architecture that incorporates patient consents at its core. The reference architecture extends the XACML authorization model, which is the de facto standard for authorization. In particular, we suggest integrating consents via a Policy Information Point (PIP) interacting with a Policy Decision Point (PDP) that enforces the suggested evaluation algorithm. An implementation of the proposal is presented at the end of the paper, together with an extensive evaluation. As a case study for the evaluation, the prototype implementation is instantiated in the context of XDS, which is an EHR proposal for cross-enterprise data sharing set forward by IHE. XDS is highly promising in the health care sector and is endorsed by key industrial players like Microsoft and IBM, which makes the illustration more relevant.

PATIENT CONSENT

Sharing patient data on a large scale has a big impact on the patient's privacy. Therefore, it is important that the patients themselves are also given the ability to determine rules concerning the access rights of their own data. This section is divided in a conceptual part and a more technical part. The first part provides an introduction to basic

22 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/chapter/integrating-patient-consent-health-access/72209

Related Content

Process Evolution in a Distributed Process Execution Environment
Pieter Hens, Monique Snoeck, Geert Poelsand Manu De Backer (2013). *International Journal of Information System Modeling and Design (pp. 65-90).*
www.irma-international.org/article/process-evolution-distributed-process-execution/80245

Non-Monotonic Modeling for Personalized Services Retrieval and Selection
Raymond Y. K. Lauand Wenping Zhang (2010). *International Journal of Systems and Service-Oriented Engineering (pp. 55-68).*
www.irma-international.org/article/non-monotonic-modeling-personalized-services/44686

A Modified Parallel Heapsort Algorithm
Hiroaki Hirataand Atsushi Nunome (2020). *International Journal of Software Innovation (pp. 1-18).*
www.irma-international.org/article/a-modified-parallel-heapsort-algorithm/256233

Issues, Limitations, and Opportunities in Cross-Cultural Research on Collaborative Software in Information Systems
Dongsong Zhangand Paul Benjamin Lowry (2009). *Software Applications: Concepts, Methodologies, Tools, and Applications (pp. 2194-2229).*
www.irma-international.org/chapter/issues-limitations-opportunities-cross-cultural/29502

LDAP Vulnerability Detection in Web Applications
Hossain Shahriar, Hisham Haddadand Pranahita Bulusu (2017). *International Journal of Secure Software Engineering (pp. 31-50).*
www.irma-international.org/article/ldap-vulnerability-detection-in-web-applications/204523