

Fine-grained Sharing of Health Records using XSPA Profile for XACML

- An Extended Abstract -

A. Al-Faresi², B. Yu², K. Moidu², A. Stavrou², D. Wijesekera^{1,2} and A. Singhal¹
{aalferes|byu3|dwijesek|kmoidu|astavrou}@gmu.edu, anoop.singhal@nist.gov,

National Institute of Standards and Technology¹,
100 Bureau Drive, M/S 8900,
Gaithersburg, MD 20899-8900.

George Mason University²,
4400 University Avenue, MS 4A4,
Fairfax, VA 33020.

Abstract

Security and privacy concerns over the handling of electronic healthcare records have received significant attention over the past few years. In response to the increase need for sharing and maintenance of personal health records many recent publications attempt to address the thorny problem of controlling access to electronic health records (EHRs) and personal health records (PHRs). These efforts include scientific and legislative work by many organizations such as NIST, AHIC, HL7, HITSP, AHIC among others. In addition, legislation such as the Health Information Privacy and Accountability Act of 1999 and ARRA-HITECH set goals to be achievable by determining the release of EHR and PHR data are those that are used in security policies used in other areas of IT security, such as subjects, objects, roles, operations and permissions. In this extended abstract, we argue for the need to re-think and re-design some of the existing policies frameworks to adhere the needs that stem from their use in a real-world health care environment.

Introduction

Due to the complex nature of healthcare data, their sensitivity to all concerned actors such as patient/their guardians, care givers, payees and external entities such as health data repositories, many more concepts need to be added to the existing repertoire of conceptual entities that need to be considered in manipulating healthcare data. Some proposed additions are due to legislative requirements that are in place to ensure the patients privacy concerns. The issues that we are addressing in our ongoing work are that of requiring patient/guardians consent in making the data available for specific purposes.

In recognition of the importance of sharing healthcare

data between two authorized entities, the OASIS has defined a Cross-Enterprise Security and Privacy Authorization (XSPA) Profile[2] for the eXtensible Access Control Meta Language (XACML) [1] where the main Use Case addresses the request-response scenario of health records between two entities cooperating in sharing information contained in personal healthcare records. At a very high level, this profile uses subjects, objects, roles, operations, permissions and purposes [3].

The clash of policies regarding consent

In the XSPA profile [2], patient/guardian consent are retained in a special repository and used as attribute, along with other attributes, such as those that identify the subjects and resources in other security policies. Nevertheless, as shown in [15,16], patients consent may change over time, depends upon the type of record and the will of the patient, and the actor responsible for the granting or altering the consent may not be the patient. The case in point is recorded in [16] where as the patient grows in age between childhood and the “age of consent” various parts of the medical records may require consent from different subjects. In addition, the age of consent is dependent on the state [16]. Therefore, our ongoing work addresses in developing XACML extensions that specify policies that would specify rules for purpose based consent granted to different objects under different environmental conditions.

Secondly, the purposes used in XSPA are listed as (1) healthcare accesses (2) emergency accesses (3) programmer accesses (4) administrator access, (4) research access (5) marketing accesses. Nevertheless, one of the stated objectives of the ARRA-HITECH act for 2013 is to support *advanced clinical processes* [9,10]. But clinical processes for potential encounters have been designed by multiple organizations and are

specified as workflows used for a large number of medical encounters [7,8]. Therefore our policies expand upon the five main purposes using these workflows. This will allow our framework to share information at a finer granularity than those currently stated in the XSPA profile.

Thirdly, HIPAA also allows a patient/guardian to obtain a list of all accesses to the patient data except in a few occasions as specified in the legislation, implying the access/release controller now has to retain and access log and permit sharing that if permitted by law and policy. Moreover, a privacy officer that is responsible for providing a reason for the denial can reject these requests [6].

The requirements stated above requires that the policies that govern fine-grain sharing of health data demand that the access controller evaluates some access while the other access rights (such as to change the consent or ownership of a data item) requires updating the policy. Doing so would create read-write conflicts in administering a complex policy framework that enforces HIPAA and ARRA-HITECH compliant policies. In addition, by enforcing these policies we want to ensure that such policies prevent intentional and accidental misuses of the workflows developed in the past [7,8]. This constitutes the main research objective of our group.

We have developed an implementation for the Administrative role base access control framework [13] where the read-write conflicts are being resolved using a locking mechanisms. As shown in [13], this does not severely degrade the performance of the policy decision point.

Among a large number of related work, we cite [12,13,15] that have addressed different aspects of purpose based access control. But to the best of our knowledge they do not directly address XSAP concerns [2] or AHIC Use cases [7,8].

References

1. eXtensible Access Control Meta Language (XACML) available at http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml.
2. Cross-Enterprise Security and Privacy Authorization (XSPA) Profile of XACML V2.0 for Healthcare Versions 1.0 committee specification available at <http://www.oasis.org>.
3. Cross-Enterprise Security and Privacy Authorization (XSPA) - WS-Trust Healthcare Profile available at <http://www.oasis.org>.
4. Role Based Access Control (RBAC) Healthcare Permission Catalog by Health Level 7, available at www.hl7.org.
5. High-Level Overview of the Health Level 7 (HL7) Consent related vocabulary including Confidentiality Codes, available at www.oasis-open.org/committees/...php/.../hl7confidentialitycodes.doc.
6. Ahmed Al-Faresi, Duminda Wijesekera and Khaled Moidu, ITEPP: IT-Enforceable Privacy Policy Model based on HIPAA Rules, submitted to the International Journal of Medical Informatics.
7. AHIC Use Cases, available at <http://www.hhs.gov/healthit/usecases/>
8. Successor to AHIC Inc, available at <http://www.ahicsuccessor.org/hhs/ahic/nsf/index.htm>
9. Robin Rayford, Meaningful use recommendations from the HIT Standards Committee, available from Health Information Technology Standards panel (HITSP), April 02, 2010.
10. Robin Raiford, Achieving the ARRA 2015 vision, personal communication, April 02, 2010.
11. J. Byun and N. Li, "Purpose based access control for privacy protection in relational database systems," *The VLDB Journal*, vol. 17, Jul. 2008, pp. 603-619.
12. J. Byun, E. Bertino, and N. Li, "Purpose based access control of complex data for privacy protection," *Proceedings of the tenth ACM symposium on Access control models and technologies*, Stockholm, Sweden: ACM, 2005, pp. 102-110.
13. Q. Ni, A. Trombetta, E. Bertino, and J. Lobo, "Privacy-aware role based access control," *Proceedings of the 12th ACM symposium on Access control models and technologies*, Sophia Antipolis, France: ACM, 2007, pp. 41-50.
14. Min Xu and Duminda Wijesekera, Towards Runtime Access Control Administration and Enforcement of Web Services, to be published in *IEEE Transactions in Service Computing*.
15. Enrico Coiera, Roger Clark, e-Consent: The design and Implementation of Consumer Consent mechanisms in an Electronic Environment, *JAMIA*, Vol II, No 2, Mar/April, 2004.
16. Whose personal Records? Creating Private, personally Controlled Health Records for Adolescent Patients, in *JAMIA* Vol 15, No 6. Nov/December 2008.