Policy Management for E-Health Records

Maritza Johnson
Department of Computer Science
Columbia University
maritzaj@cs.columbia.edu

Steven M. Bellovin
Department of Computer Science
Columbia University
smb@cs.columbia.edu

Abstract

The ability to share electronic health records across healthcare providers plays a large role in the prediction that electronic health record systems will revolutionize the healthcare industry in the United States. Sharing health records raises the obvious question of how to implement access control in this distributed domain. The answer to which is not simply an architecture that can enforce the necessarily complex access control policies, but also knowledge of who will manage the policies and how they will manage them. Achieving this goal requires user-centered design methods and empirical evaluations of interfaces that facilitate fine-grained policy management. Policy management is a task that is difficult for users but is essential to an electronic health record system that permits sharing among users.

1 Introduction

Electronic health record (EHR) systems are currently deployed or are being deployed in a number of large countries *e.g.,* the United Kingdom, Canada, Australia, and the United States. Recently, the United States enacted new legislation that provides $18 billion dollars in incentives to speed the adoption of EHR systems [9]. The stated goal is to digitize the health records of every American by 2014. The ability to share health records between healthcare providers is projected to cut healthcare costs dramatically. Researchers have responded to this burgeoning demand by investigating the security requirements and design of such a system, while others are investigating the usability issues associated with adopting EHR systems and other health information technology solutions. Neither of these approaches is addressing the usability of managing the access control policies.

For EHR systems to be successful it is critical that they are able to enforce an access control policy that states who can access what information and under which conditions. One aspect of implementing access control for EHRs is designing systems that are flexible enough to enforce a large range of access control policies. Expressibility is of concern due to the large number of rules, roles, and objects that will be needed (a case study of EHR usage in England had approximately 310 rules and 58 roles [1]). Proposed solutions include alternative database access protocols [7], systems that supplement preventative access control with audit-based access control [3], and solutions that support declarative policies using a trust management system [1]. This work is certainly needed but immediate attention must be given to who will manage the access control policies. Indeed, audit-based access control will likely useful in this dynamic environment where users cannot always predict who will need access to what and when. However, someone will need to specify a base set of preventative rules since an audit-based system, one that primarily relies on logging and accountability, will not offer sufficient protection against unauthorized access. It will also be necessary to limit who is trusted to "break the glass" and under what conditions. These are access control decisions and policies that must be authored by a person.

The fact that a person is needed to author the access control policies implies the access control system must have a strong usability component. This will be a requirement regardless of whether the responsibility of managing access control falls on an administrator, a healthcare provider, or the patient. It will also be a requirement regardless of where the record is stored. With personal health record (PHR) systems, the patient maintains most of the data stored in the record and there are features that allow the patient to share their record with family members, healthcare providers, and other relevant parties. In this case, the patient will manage their access control policy.

Policy management is a difficult task for users and even administrators need usable tools. Policy management has been a topic of interest in the usable security community, where the primary focus has been on file access control and privacy settings, progress has been made but a solution for fine-grained access control has not been identified.

2 Usable Policy Management

The user who fills the role of the policy author is responsible for creating, editing, and managing policies. This means the user must have a clear understanding of the policy goals and be able to formulate how to achieve the goals using the policy language or interface provided. They must have a way to verify they specified the policy correctly, or as closely as possible, and they must have a way to quickly get an overview of the effective policy.

2.1 File access control and Privacy Settings

Currently, the average user might have experience with file-sharing but is more likely to have encountered a policy management task when using a social networking website. Users have a difficult time reading and modifying file permissions though changes to the interface can improve perfor-

mance [8]. Empirical evaluation has shown that most users share files via email attachments [10]. Even users who know how to use file-sharing tools use email as a fallback when they have trouble [2]. Online social network users have more incentive to manage their privacy settings since they can protect their personal data, but most users accept the default settings [6]. Relying on default settings could be a reasonable option, but this assumes the default settings are useful.

These results have interesting implications for EHR policy management. It is possible that users do not have enough incentive to manage file permissions and privacy settings, but will put more effort toward managing their EHR. Or, existing tools are too difficult to use and fail to demonstrate enough utility to encourage users to learn to use them correctly [4].

2.2 EHR Systems

Endusers have never been required to manage an access control policy for data as sensitive as medical information. Because the data is more sensitive than data shared on social networking sites, users should be more motivated to manage the access control policies carefully. Prior research introduced tools that improve usability on small policy authoring tasks. Guided natural language and structured entry lists are more usable for policy authors compared to unstructured natural language [5]. And tools to visualize the effective policy that help users understand file access control policies [8]. However, more advanced methods of managing access control are necessary.

Policy templates composed of smart policy elements offer a new approach that has not been explored. Policy elements are objects that represent the elements of a system that are controllable by a policy. Policy templates are natural language policy statements composed of policy elements. The policy author creates new policies by selecting values for each policy element. For EHRs the policy elements will include: an object for each role/user who can access a record, an object for each data item in the EHR, an object for each possible action in the system, and objects to represent the conditions under which users can access information. Policy elements can be augmented to include risk information to be communicated to users and metadata that indicates which combinations of values are valid.

In existing EHR systems users are expected to self-police their access based on the knowledge that the system is auditing how they access patient's medical records. Fine-grained access control management tools are required to prevent hospitals from using this technique.

The development of tools for the visualization of the effective policy is important. Policy authors need a usable overview of the policy and endusers must be able to determine who has access to what. Expandable Grids was shown to be useful for representing the effective policy for file access control[8]. Further research is needed to determine the best method of displaying a large number of rules. The number of rules in an EHR policy is likely to be large so it is important to research effective methods of easily determining what access a specific user has, or which users have access to a piece of data of interest.

3 Conclusion

Access control is paramount to the success of EHR systems. Usable fine-grained access control is a key requirement that needs immediate attention. Policy management has proven to be a difficult task even in domains where the policies are less complex than in the healthcare domain.

4 References

[1] M. Y. Becker and P. Sewell. Cassandra: Distributed access control policies with tunable expressiveness. *Policies for Distributed Systems and Networks, IEEE International Workshop on*, 0:159, 2004.

[2] B. Dalal, L. Nelson, D. Smetters, and N. Good. Adhoc guesting: When exceptions are the rule. In *UPSEC '08: Usability Psychology and Security*, 2008.

[3] M. Dekker and S. Etalle. Audit-based access control for electronic health records. In *Proceedings of the Second International Workshop on Views on Designing Complex Architectures (VODCA)*, pages 221–236, Amsterdam, September 2006.

[4] M. Johnson, S. M. Bellovin, R. W. Reeder, and S. Schechter. Laissez-faire file sharing: Access control designed for individuals at the endpoints. In *NSPW '09: Proceedings of the New Security Paradigms Workshop*, pages 1 – 10, September 2009.

[5] J. Karat, C.-M. Karat, C. Brodie, and J. Feng. Privacy in information technology: Designing to enable privacy policy management in organizations. In *International Journal of Human-Computer Studies*, volume 63, pages 153–174. Elsevier, 2005.

[6] B. Krishnamurthy and C. E. Wills. Characterizing privacy in online social networks. In *WOSP '08: Proceedings of the first workshop on Online social networks*, pages 37–42, New York, NY, USA, 2008. ACM.

[7] L. E. Olson, C. A. Gunter, and S. P. Olson. A medical database case study for reflective database access control. In *ACM Workshop on Security and Privacy in Medical and Home-Care Systems (SPIMACS)*, pages 41–51, 2009.

[8] R. W. Reeder, L. Bauer, L. F. Cranor, M. K. Reiter, K. Bacon, K. How, and H. Strong. Expandable grids for visualizing and authoring computer security policies. In *CHI '08: Proceedings of the SIGCHI conference on Human factors in computing systems*, pages 1473–1482, NY, NY, USA, 2008. ACM.

[9] U.S. Congress. American recovery and reinvestment act. `http://www.recovery.gov/About/Pages/The_Act.aspx`.

[10] T. Whalen, D. Smetters, and E. F. Churchill. User experiences with sharing and access control. In *CHI '06: CHI '06 extended abstracts on Human factors in computing systems*, pages 1517–1522, New York, NY, USA, 2006. ACM.