Purpose Management and Enforcement for Sensitive Private Data in Open Environments

Rath, Thavy Mony Annanda; Colin, Jean-Noël

Publication date:
2012

Document Version
Early version, also known as pre-print

Purpose Management and Enforcement for Sensitive Private Data in Open Environments

Annanda Thavymony RATH, rta@info.fundp.ac.be
Jean-Noël COLIN, jean-noel.colin@fundp.ac.be
Faculty of Computer Science, University of Namur,
Belgium

Abstract

This paper provides an overview of our research including the specification of research, the primary result we achieved so far, and the remaining questions to be addressed. We set ourselves in the field of secure processing of sensitive private nomad data in open (distributed) environments. The goal of the research is to investigate the role and impact of "purpose" in authorization process (access as well as usage control) and define a mechanism to manage and enforce them. The research includes: (1) study, analyze, and clear the meaning of purpose, (2) management of purpose binding of data, (3) study the possibilities to recognize purpose binding and enforcement, and (4) clear the meaning and impact of personal relationship, context on purpose in authorization process.

1.1 INTRODUCTION

Purpose[1]of access is one of the core concepts in privacy, which considers the requester's intent as a factor in making access control decision. It has been also considered in major privacy legislations[2] where the processing of sensitive private data is bounded to the specific purpose and the excessive use of them are prohibited. With this regard, in any processing environment dealing with such data requires great attention to make sure that system can provide adequate data processing security aligning with privacy legislation. This leads to the necessity of the effective management of purpose binding of data (including the recognition of purpose biding data) and enforcement.

The implication of "purpose" in authorization process (for private data) has been actively studying. It is raised and argued in many literatures as an important entity used to control access to sensitive private data. Byun et al [1] proposed a purpose-based access control of complex data for privacy protection, a model that relies on the well-known RBAC [2] access control model as well as the notion of conditional role that is based on the notion of role attribute and system attribute. In their paper, they provide also a general-purpose tree applied in complex data management system and the solution to address the problem of how to determine the purpose for which certain data are accessed by a given user. Other research concerning purpose is done by Ni.Qun et al [4]; they proposed a P-RBAC (Privacy-aware RBAC), in which they extended the concept of

---

[1] In the natural language, "purpose" often refers to an action (or a set of actions) or the name of the abstract actions that need to be performed following the access of data

[2] Privacy legislations: the 95/46/EC Directive, U.S Privacy Act (1974), and Canada's Federal Privacy Act (1983)

RBAC model by adding three entities that require expressing the access control policy for sensitive private data. Those entities are purposes, conditions, and obligations. They argue that purpose is the important entity (it can not be missed) and serves as a key factor in determining the access to sensitive data.

While the previous researches focused mostly on how to express and represent “purpose” in the access policy, the management and enforcement of "purpose" have been poorly studied. Thus, by observing the lack of the study on purpose management and enforcement in open environment, we willing to contribute our research in this area. We focus our research in three main points. (1) Study, analyze, clear the meaning of purpose, and the management of purpose binding of data; (2) the purpose enforcement; and (3) the study of the impact of the personal relationship, context on purpose for sensitive private data.

The rest of paper is organized as following. Section 2 provides the definition and scope of the "purpose". Section 3 talks about the purpose management and enforcement, in this section, we also discuss our proposed purpose enforcement structure. Section 4 is the past achievements and future work while Section 5 is the conclusion.

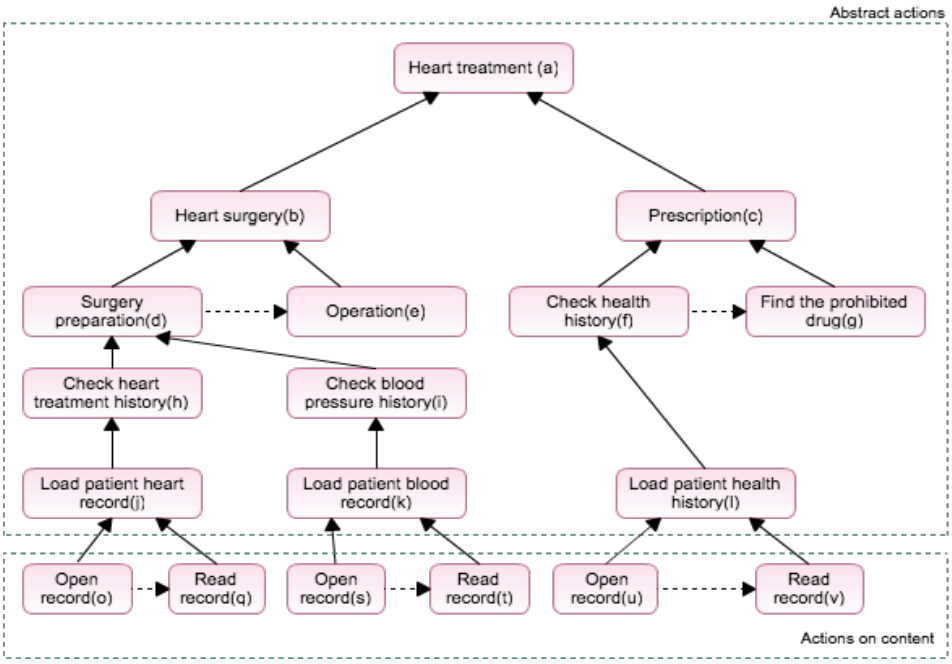

Figure 1: Example of purpose graph in healthcare where dashed arrows represent purpose as ``future action" and solid arrows represent “purpose” as “high-level action”. They are read from bottom up for solid arrows (e.g, “surgery preparation” is a high level action of “check heart treatment history”). Dashed arrows are read from left to right (e.g, “operation” is a future action of “surgery preparation”)

1.2 DEFINIATION AND SCOPE OF PURPOSE

In dictionary, “purpose" is defined as “the object toward which one strives or for which something exists; an aim or a goal”. However, by observing how purpose is used in the natural language reveals that purposes often refer to an abstract or a set of abstract actions. For example, accessing patient's health record for the purpose of treatment,

research, insurance, etc. all of which are names of some abstract actions. To our observation, purpose can be classified into two types: purpose as high-level action and purpose as future action (Figure 1).

Purpose as a High-Level Action[3], in some contexts, purpose refers to a more abstract, or semantically higher-level action in a plan. Thus, doing something for some purpose; actually means doing it as a part, or a sub-action, for that higher-level action. For example, when Bob checks some patient's blood pressure for the purpose of heart surgery, it means that checking the blood pressure is a part of a more complex and abstract action of heart surgery. Similarly, when it is said the surgery is performed for the purpose of treatment, it is because the high-level action of medical treatment includes surgery as a part. As presented in Figure 1, the abstract action "purpose" (a) is considered as the high level action of "(b) to (v)".

Purpose as a Future Action, in some contexts, purpose is used to indicate that an action is performed as a prerequisite of another action in future. For example, when Bob withdraws money from a bank account for the purpose of paying the bills, it means the former action is done as a prerequisite to performing the latter. Another example as presented in Figure 1, when a doctor does the surgery preparation for a purpose of operation, it means the former action "surgery preparation" is done as a prerequisite to performing the later action which is "operation". In Figure 1, (e)(g)(q)(t)(v) are considered to be the future action of (d)(f)(o)(s)(u) respectively.

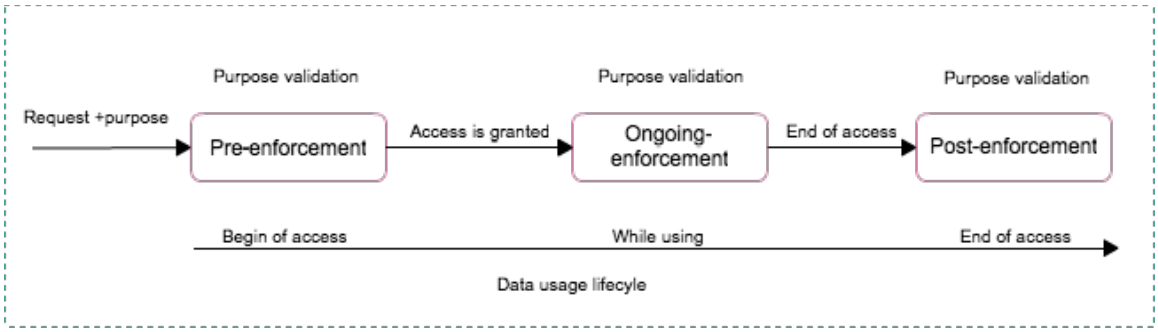

Figure 2: Example of purpose enforcement structure

1.3 PURPOSE MANAGEMENT AND ENFORCEMENT

The main difficulty in purpose enforcement is how to identify the purpose of an agent when it requests to perform an action. Some common proposed mechanisms for purpose management and enforcement are self-declaration in which the agent explicitly announces the purpose of data access and role-based enforcement in which the purpose is identified based on the agent's role in the system. The first method obviously cannot stop a malicious agent from claiming false purposes. The second method has been criticized to

[3] Common terminology Low-level actions such as read, write, etc are well known and common across many domains with clear and standard meanings. More complex and abstract actions like surgery; marketing, etc. can be taken from standard vocabularies that exist in many domains such as clinical systems in healthcare.

be inefficient in capturing purpose of an action since roles and purposes are not always aligned and members of the same organizational role may practice different purposes in their actions. Therefore, identifying the purpose of an action, or verifying a claimed purpose remains an open question. With this regard, we would like to set ourselves on purpose management and enforcement. Within this framework, we investigate into three enforcement states, we term, pre-enforcement, ongoing-enforcement, and post-enforcement of purpose. To our observation, we can enforce “purpose” in three different circumstances (phases) as presented in Figure 2, before access is granted, while using content, and at the end of content usage; however, the three enforcement phases require different mechanisms to handle them.

Pre-enforcement of purpose refers to a mechanism allowing system to validate the purpose before granting access to data. In this point, we work on defining or formalizing a mechanism used to efficiently validate the declared purpose. This includes also the infrastructure/system architecture to support the defining mechanism.

Ongoing-enforcement of purpose refers to a mechanism allowing system to continuously control purpose of usage during the usage period. It checks if the actions performed and the requesting actions are conformed to the declared purpose.

Post-enforcement of purpose refers to a mechanism allowing system to validate the processing of data and identify if the usage of data was inline with the requested-purpose or otherwise. In this part, we work on defining the mechanism that is able to trace and validate the usage of data.

Our preliminary conclusion is that the proposed enforcement structure would provide a full control over data usage because enforcement takes place over the entire lifecycle of data usage; hence, the immediate quest is the mechanism to effectively enforce the three phases of purpose validation.

1.4 PAST ACHIEVEMENTS AND FUTURE WORK

Privacy protection is a major issue of the systems dealing with sensitive private data, the most well known of which are the healthcare information system and social network. As our research focus is on this type of data and processing environment, we started our work from this point by looking at distributed healthcare information system. We conducted a case study on Walloon Healthcare Network (WHN). Following the work on WHN, we worked on Digital Right Management system; the aim is to find out if the existing system is sufficient to be used for the protection of sensitive private data in the identified environment. Following the DRM system, we worked on right expression language and access as well as usage control model.

The latest study we have conducted relates to "purpose", the study includes the semantic foundation of purpose for privacy policies to access control model based on purpose and its expression language. We went deeper into the policy expression languages like XACML, ODRL, or EPAL to find out if these languages can be used to express “purpose”. Our study shows that those languages are capable to support “purpose” expression; however, the enforcement of purpose binding policy is still a challenge.

Concerning “purpose” enforcement, we conducted the survey on existing enforcement techniques for access as well as usage control [3] and we found that most techniques can

address only a partial problem in “purpose” enforcement; a more suitable approach is required. Thus, we settle in this area; talking about “purpose enforcement”, the main difficulties are: How to identify/verify the purpose of an agent when it requests to perform an action? And how to ensure that the usage of data does not exceed the declared purpose? Thus, two important points need to be addressed. (1) System architecture, taking distributed healthcare as the main application domain. (2) The mechanisms for purpose validation for the three enforcement phases as mentioned in previous section.

In relation with purpose, our following research focus is to study the impact of the personal relationship, context on purpose for sensitive private data. This motivates by the fact that social-network and healthcare system dealing with sensitive private data seems to reflex the concept of personal relationship in their access as well as usage control management. Our research in this part is to define a general access control model termed as "privacy-aware relationship-based access control model " and to prove that such model can provide a promising result as compared with other access control model such as P-RBAC if deployed in the above-mentioned system environments.

1.5 CONCLUSION

We have presented in this document, the research objective and the progress we achieved so far. With the main objective of managing and enforcing ``purpose'' in privacy policy for private nomad data in open environment, we propose the enforcement structure as presented in section 3. Through a preliminary study, it seems much can be achieved by using this approach. This approach allows us to have a full control over the data usage from earlier access (pre-enforcement of purpose) to end of access (post-enforcement of purpose).

REFERENCES

[1] Byun Ji-Won, Bertino Elisa, and Li Ninghui (2005). Purpose based access control of complex data for privacy protection. In Proceedings of the tenth ACM symposium on Access control models and technologies, SACMAT ’05, pages 102–110, New York, NY, USA. ACM.

[2] D.F.Ferraiolo, R.Sandhu, S.Gavrila, D.R.Kuhn, and R.Chandramouli. (2001). Proposed NIST Standard for Role-Based Access Control. In ACM Transactions on Information and System Security, pages 4(3):222–274.

[3] Katt Basel, Zhang Xinwen, Breu Ruth, Hafner Michael, and Seifert Jean-Pierre (2008). A general obligation model and continuity: enhanced policy enforcement engine for usage control. In Proceedings of the 13th ACM symposium on Access control models and technologies, SACMAT ’08, pages 123–132, New York, NY, USA. ACM.

[4] Ni.Qun, Bertino Elisa, Lobo Jorge, Brodie Carolyn, Clare-Marie Karat, and Trombeta Alberto (2010). Privacy-aware Role-Based Access Control. ACM Transaction Information and System Security, 13:24:1–24:31.

[5] Park, Jaehong, and Sandhu Ravi (2002). Towards usage control models: beyond tra- ditional access control. In Proceedings of the seventh ACM symposium on Access control models and technologies, SACMAT ’02, pages 57–64, New York, NY, USA. ACM.

[6] Park, Jaehong, and Sandhu Ravi (2004). The uconabc usage control model. ACM Trans. Inf. Syst. Secur., 7:128–174.