A Purpose Model and Policy Enforcement Engine for Usage Control in Distributed Healthcare Information System

Annanda Thavymony Rath and Jean-Noël Colin
PReCISE Research Center, Faculty of Computer Science, University of Namur, Namur, Belgium

Keywords: UCON (Usage CONtrol), e-Health, Purpose, Policy Enforcement Engine.

Abstract: This paper addresses two issues: the purpose model designed for distributed healthcare and the purpose-based usage policy enforcement engine based on our purpose-based UCON (the extended UCON model). UCON has been proposed and applied to support security requirements in different computing environments such as resources sharing in collaborative computing systems and data control in remote users or platforms, but apparently absent in its core model is "purpose", which is important for formulating a more sound privacy sensitive policy. In this paper, by observing a lack of comprehensive enforcement mechanism for purpose, we extend the UCON core model to explicitly support purpose expression and then propose a usage purpose enforcement engine, particularly for ongoing-enforcement, applied in distributed healthcare information system.

1 INTRODUCTION

Health record is important in the course of a treatment process for the proper continuing care for the patient. Over last decade, with the increase of the electronic materials in healthcare and the improvement of network and system, "electronic health records" has become increasingly common and widespread to replace the traditional paper based record. However, making the information available electronically poses new security concerns (Li, W. and Hoang, D., 2009) (Rath and Colin, 2012a), especially when sharing them between different healthcare institutions where the control of usage is required.

In our work, we deal with the patient privacy preservation issue, particularly, access and usage security requirements in healthcare system. Our work is under the scope of Walloon Healthcare Network (Rath and Colin, 2012b). WHN is a project that aims at providing an electronic healthcare facility to patients in Walloon Region, Belgium, by joining together all healthcare institutions, clinics, and also physicians and allow exchanging patient's record when needed. Below are a summary of the security requirements for WHN.

(1) Only authorized users are allowed to access patient's record. Users need to have also patient's consent in order to be able to access to or use patient's record. (2) Access or usage rights are based on the roles of users such as users in role healthcare professional (physician, nurse, or pharmacist), patient's guardian, or patient's trusted-person. (3) Conditions: patient's record can be stored at doctor's machine or other authorized devices only for a specific time period. (4) Obligations: every access to content, user needs to notify patient. The notification is done before and after the session is started. The log of usage activities is also required during the usage session. (5) Purposes: the use of patient's record must be for the specific purposes.

With the requirements above, we can see clearly the need of control over the usage of patient's record and the involvement of purpose in usage decision authorization. Concerning the current UCON core model (Park and Sandhu, 2004), it does not clearly address the purpose expression as well as its enforcement mechanism. To meet these requirements. UCON core model and its policy expression must be extended. We extend it by adding "purposes" to its core model. We argue that purpose of usage needs also to be checked and enforced before, during, and after the usage of record. This is to make sure that user is using data in accordance to the claimed purpose; hence, "purposes" should be considered as one of the principle components in UCON core model.

The rest of the paper is organized as following. Section 2 presents related work. Section 3 talks about the purpose model. Section 4 presents purpose enforcement structure. We present UCON model and its extension in Section 5. Section 6 presents purpose

Thavymony Rath A. and Colin J..
A Purpose Model and Policy Enforcement Engine for Usage Control in Distributed Healthcare Information System.
DOI: 10.5220/0004223201740180
In *Proceedings of the International Conference on Health Informatics* (HEALTHINF-2013), pages 174-180
ISBN: 978-989-8565-37-2

enforcement engine and its architecture. Finally, we conclude and present our ongoing work in Section 7.

2 RELATED WORK

(Ji-Won et al., 2005) proposed a purpose-based access control of complex data for privacy protection, a model that relies on the RBAC (Ferraiolo et al., 2001) access control model as well as the notion of conditional role which is based on the notion of role attribute and system attribute. In their paper, they defined 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.

(Mohammad et al., 2011) defined a semantic model for purpose, based on which purpose-based privacy policies can be expressed and enforced in a business system. The proposed model is based on the intuition that the purpose of an action is determined by its inter-related actions, which are modeled in the form of an action graph. A modal logic and model checking algorithm are developed for formal expression of purpose-based policies and verifying whether a particular system complies with them.

(Park, J. and Ravi, S., 2002) proposed the usage control model, $UCON_{ABC}$ (Park and Sandhu, 2004) in particular, that integrates Authorization (A), oBligation(B), and Condition (C) into usage decisions. $UCON_{ABC}$ supports two features that distinguish it from the traditional access control models: decision continuity and attribute mutability. Concerning decision continuity, it is able to distinguish between decisions made before access is started and decisions taken during the access session. While considering the mutability factor, update actions are introduced before, during, or after an access session.

Concerning enforcement, (Katt, B. et al., 2008) proposed the extension of $UCON_{ABC}$ with continuous control usage sessions for expressing the ongoing-check obligation. They also proposed the general, continuity-enhanced policy enforcement engine for usage control applied particularly to obligation.

3 PURPOSE MODEL

Observing how purpose is used in the natural language reveals that purposes often refer to an or a set of abstract actions. For example, accessing patient's health record for the purpose of treatment, research, etc. all of which are names of some abstract actions. (Mohammad et al., 2011) classified "purpose" in two types: purpose as high-level action and purpose as future action (Figure 2).

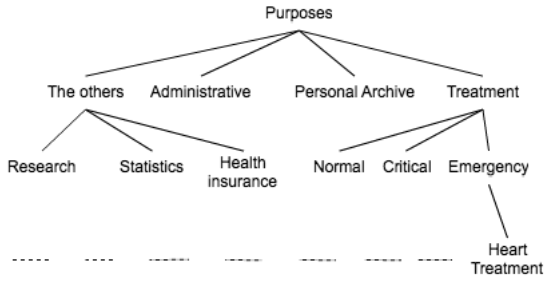

Figure 1: A simplified high level purpose tree in e-health system. Dashed-line represents more purpose elements in each sub-categories. The detail example on "heart treatment" purpose can be found in Figure 2.

Purpose as a High-Level Action 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. As presented in Figure 2, the abstract action "purpose" (a) is considered as the high level action of "(b) to (v)".

Purpose as a Future Action is used to indicate that an action is performed as a prerequisite of another action in future. For example as presented in Figure 2, 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 2, (e)(g)(q)(t)(v) are considered to be the future action of (d)(f)(o)(s)(u) respectively.

Based on the definition of purpose above, we model the purpose in e-health system as the inter-related actions and has the hierarchical structure as presented in Figure 1 and Figure 2. The proposed structure is simple and appropriate in common healthcare information system. The details of them are presented as following.

1) "Treatment" describes a purpose of healthcare professional, particularly, doctor to use data for patient treatment. The treatment purpose can be divided into sub-categories as following. "Normal " is defined for consented-healthcare professional in case they want to access and use patient's record for a normal treatment (e.g., a visit by patient for a particular illness or yearly medical check). "Critical" is defined for the use of content in case of the urgent operation or treatment of patient. It is important to note that "emergency" is different from "critical" in such a way that

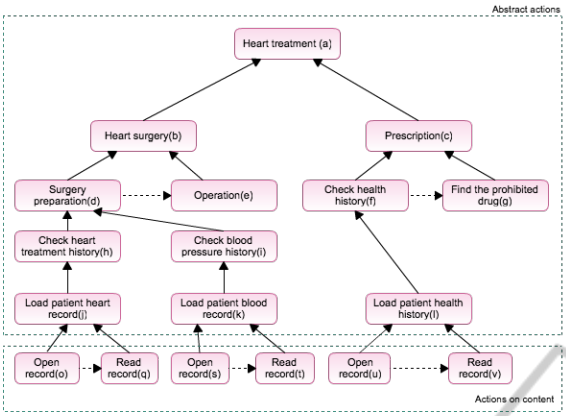

Figure 2: Example of purpose graph in healthcare where dashed arrows represent purpose as “future action” and solid arrows represent ”purpose” as “high level action”. They are read from bottom up for solid arrows (e.g, “surgery preparation” is a high level action of “check heart treatment history”). Dashed arrows are read from left to right (e.g, “operation” is a future action of “surgery preparation”).

in critical situation, rights applied to patient’s data can not be revoked and only the users who have patient’s consent can access and use data. “Emergency” is defined for emergency situation, in this case, all rights applied to patient’s data can be revoked. ”Emergency” is different from ”critical” in such a way that in emergency situation, even unconsented-healthcare professional can also access patient’s record.

2) Personal Archive is defined for patient or consented-healthcare professional in case they want to access and use the patient’s record for their personal archive.

3) Administrative is defined for healthcare institution personnel in case they want to access data for the administrative work (e.g., accessing information in prescription for delivering the drugs).

4) ”The others” is defined for any purposes that do not relate to treatment process. This ranges from research to other purposes required by external entity.

- Research: this purpose of usage is defined for any authorized entity or organization to access patient’s record for the purpose of medical research.
- Statistic: this purpose is defined for the healthcare institution to be able to access patient’s record to generate the statistical report for the defined purposes.
- Health Insurance: This purpose is defined for the access by authorized external entity, for instance, health insurance company.

Figure 2 presents a detail example of a structure of purpose named ”heart treatment”. It can be considered as the general purpose structure. However, It is understood that the elements in the structure may be different from purpose to purpose. The study of each purpose structure should be done as case by case basic.

4 PURPOSE ENFORCEMENT STRUCTURE

The main difficulty in purpose enforcement is how to identify the purpose of an agent when it requests to perform an action. To our observation,“purpose” can be enforced in three different circumstances (phases), before access is granted, while using content, and at the end of content usage.

Pre-enforcement of purpose refers to a mechanism allowing system to validate the purpose before granting access to data.

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 complied with the claimed purpose.

Post-enforcement of purpose refers to a mechanism allowing system to validate the processing of data after using it. It identifies if the usage of data was inline with the requested-purpose or otherwise. It is a pro-active mechanism.

With the above consideration, we see that to ensure the correctness of data utilization, the purpose in three states must be maintained, particularly, the ongoing-enforcement. With the above illustration, we argue that in order to maintain and to make sure that user is using data in the right direction, the three verification states are required for purpose validation: pre, ongoing, and post. Therefore, we can define our purpose as a tuple of PU that consists of 4 elements as following.

PU = (P, WHEN, DURATION, VALIDATION)

Where “P” is a purpose of data usage claimed by subject. “P” has the hierarchical property. If data is assigned for a high level action purpose “P”, any purposes that are the low levels actions to “P” is automatically permitted. “ WHEN” tells when the purpose should be check, it can be ”pre, ongoing, or post”. “DURATION” is the time period to check the validation of purpose (e.g., during the emergency treatment session). “VALIDATION” expresses the mechanism used to check the validity of the purpose claimed by subject.

As in our model, we require also the continuous (ongoing) check of purpose like obligation presented

by (Katt, B. et al., 2008); hence, we adopt their idea for the extension of the state transaction of original UCON model (Zhang, X. et al., 2005). Basel et al proposed an extended UCON state transactions to support the ongoing check on obligation. The difference between our work and theirs is that, they apply this state transaction for ongoing obligation check, for us, we apply it for ongoing purpose check.

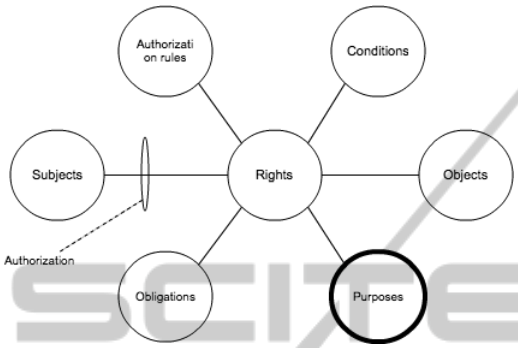

Figure 3: UCON model components with purposes extension.

5 UCON MODEL AND ITS EXTENSION

Usage Control (UCON), proposed by (Park, J. and Ravi, S., 2002) , is a model that encompasses traditional access control, trust management, and digital rights management and goes beyond them in its definition and scope. UCON enables fine-grained control over usage of digital objects than that of traditional access control policies and model. UCON model consists of six components (as illustrated in Figure 3, except "purposes" in darker color), such as subjects, rights, objects, conditions, authorization rules, and obligations.

"Subjects" are the entities associated with attributes, and hold and exercise certain rights on object. The attributes are the properties of subjects that can be used in authorization process. "Objects" are the entities that subjects hold rights on. Objects can be anything ranging from the digital multimedia content (e.g., sons, movies, ...) to the system resources. In general, objects are associated with attributes that can be used in the authorization process as that of subjects. "Rights" are the privileges that subjects can hold on an object. Rights consist of a set of usage functions that enable a subject's access to object. Rights associates subjects and objects. In general, rights can be viewed as the usage actions allowed to perform on object. "Authorization" rules are a set of requirements that should be satisfied before allowing subjects access to objects or use of objects. There are two types of authorization rules: Rights-related Authorization Rules (RAR) and Obligation-related Authorization Rules(OAR). The RAR is used to check if subject has valid privilege, for instance, subject's role. The OAR is used to check if subject has fulfilled or agreed to fulfill their obligation, for instance, notify to patient or agreed on logging the usage activities. "Conditions" are a set of decision factors that the system should verify at authorization process along with authorization rules before allowing the use of digital data, for instance, number of views, the number of copy, or duration of use. "Obligations" are the mandatory requirements that a subject has to perform before or after obtaining or exercising rights on an object.

As illustrated in Figure 3, original UCON model consist of 6 components, we propose to extend it by adding "purposes" component into the model to make it suitable and more sound to express the policy that requires "purpose expression". To adjust to the change of the entity in the core UCON model, we introduce another type of authorization rules over the two existing rules (RAR and OAR). We term it as "PAR: Purpose-related Authorization Rules".

The PAR is used to check if the purpose claimed by subject is valid. It is worth noting that our extension is based on the principle that a general model should be able to cover and support as many feasible security policies for different system environments as possible.

6 USAGE ENFORCEMENT MODEL

In this section, we present in detail the usage enforcement model with the corresponding meta-model applied in distributed healthcare information system. The enforcement model focuses on the system architecture and functional modules to illustrate how the policy model can be achieved. The proposed architecture considers all the UCON core model and the extension we propose that includes "purpose" to support the policy expression required particularly for distributed healthcare information system. It is important to note that our proposed model is the extension of the model proposed by (Katt, B. et al., 2008) by introducing a new Purpose Decision Function (PDF) module into the decision point module. Another extended component is Information for PDF "IPDF" that is designed to be used particularly in distributed healthcare. We will explain in detail the relation between them in the following section.

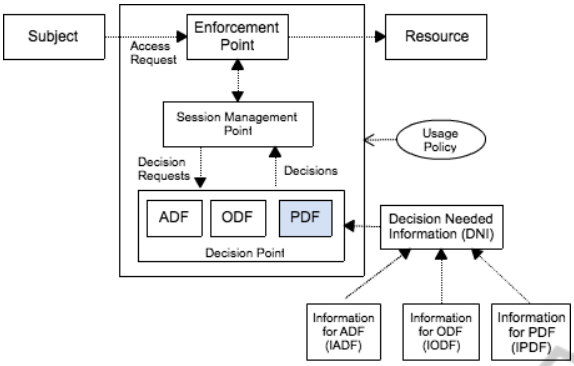

Figure 4: Usage control enforcement model with purpose extension.

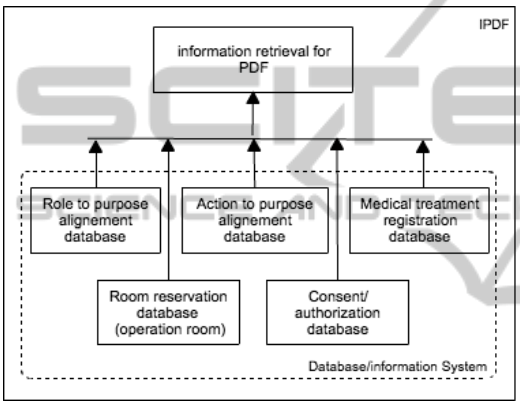

Figure 5: The detail components of IPDF.

6.1 Usage Control Enforcement Model

As illustrated in Figure 4, the model consists of three core components: Enforcement Point (EP), Decision Point (DP), and Session Management Point (SMP) with other supplementary modules like Usage Policy and Decision Needed Information(DNI) or Information Point(IP).

1. DP is responsible for making the required decision during a usage control session. It consists of three decision-making components such as ADF, ODF, and PDF (a new decision-making component, which is used to check the validity of the purpose claimed by subject). These three modules are detailed as follows:

   "ADF" handles the attribute-based access decision during a usage session. Attributes can be either subject, object, or environment attributes. The information required by ADF is retrieved from "IADF" module. "ODF" makes the decision whether a specific obligation has been fulfilled. "DP" checks the fulfillment of an obligation by transforming it into an ordered sequence of system actions, which should be defined for all obligations. During the obligation fulfillment check process, in case, the DP requires more information needed in obligation evaluation process, it contacts "IODF". "PDF" makes the decision whether a purpose is valid. Whenever there is a request, DP checks the request based on the claimed-purpose by subject. To validate the usage purpose, PDF contacts "Information for PDF (IPDF)" module through DNI for validation.

2. EP handles the requests from subject and forwards those requests to decision point trough session management point. If the usage request is granted by DP, then EP allows subject to access resource, else, the denied message is sent out to subject.

3. SMP is the module that manages individual usage sessions. This includes requesting required decision(s) from concerning modules (ADF, ODF, or PDF) in each state during the usage session.

In addition to the three core components, the "Decision Needed Information (DNI)" is a module that is responsible for supplying the information needed in decision process for a particular decision function (e.g., information for ADF, ODF, or PDF).

- IADF module is responsible for retrieving the information concerning the subject, object, and the system environment attributes.
- IODF module is responsible for retrieving all the information required during the obligation checking process.
- IPDF module is responsible for providing the information concerning the validity of the usage purpose claimed by subject. This module, as presented in Figure 5, consists of 5 important components.

  (1) "Role to purpose alignment" provides the information concerning the alignment between the requester's role and the purpose of access. (2)"Action to purpose alignment" provides the information concerning the alignment between the actions on object and the purpose. (3)"Medical treatment registration", in general, patient needs to register for the medical check up, the registration information can be used to prove if the purpose claimed by the requester is inline with the treatment of the patient. (4)"Room reservation (operation room or emergency room) provides the information concerning the room reservation for each operation. This module is designed as the source of information in case of emergency situation to validate the claimed-purpose. (5)"Consent/authorization" provides the information about who is particularly

authorized for which purposes. This module is administrated by the trusted entity that has the authority to align a particular user or a group of user to the particular purposes.

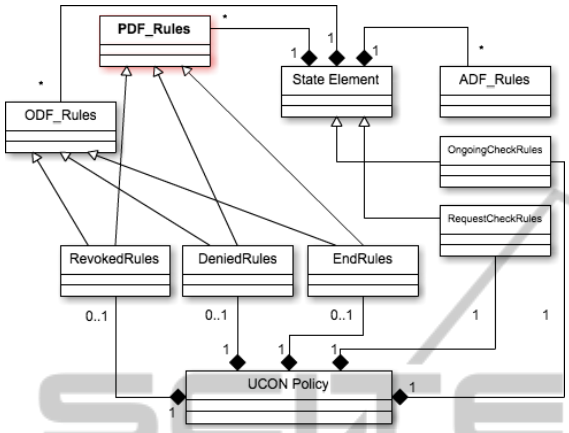

Figure 6: UCON enforcement meta model with purpose extension.

6.2 Enforcement Meta Model

In this section, we present the usage control enforcement meta-model for UCON enforcement, as presented in Figure 4, which is able to configure the enforcement engine with rules needed for each state in usage sessions. It is important to note that, this meta-model is the extension of the model proposed by Basel et al (Katt, B. et al., 2008). We extend the existing model by introducing a PDF_*Rules* into the existing model making it to be suitable for expressing policy that involves ongoing-check purpose expression. As illustrated in Figure 6, the core elements of the meta-model are the ADF_*Rules*, ODF_*Rules*, and PDF_*Rules*.

- ADF_*Rules* are the rules representing ADF function of the enforcement model (e.g., the authorization and condition predicates of a UCON policy).
- The ODF_*Rules* are obligation rules representing ODF functions of the decision point.
- PDF_*Rules* are the purpose rules representing PDF function of the decision point.

In addition to the three rules component above, there are other rules component that are applied for different states in processing user's request such as RequestCheckRules, OngoingCheckRules, DeniedRules, RevokedRules, and EndRules.

"RequestCheckRules" is applied at the RequestCheck state when subject requests to access the object. "OngoingCheckRules" is applied at the OngoingCheck state during the usage session, "DeniedRules" is applied at Denied state when the requestCheckRules is fail. "RevokedRules" is applied at revoked state, revoked state happens during the usage session when the usage rights no longer valid (e.g., the obligation is not fulfilled or purpose of usage is invalid) "EndRules" is applied at End state.

7 CONCLUSIONS AND FUTURE WORK

In this paper, first, we modeled the purpose for distributed healthcare and then we extended $UCON_{ABC}$ to support "purposes" expression by introducing purpose as one of its core components. Second, a $UCON_{ABC}$-based solution usage control enforcement model is introduced. This model is designed to enforce the purpose-based usage policy in the distributed healthcare environment. Following this work is the implementation of the proposed model by developing a prototype applied particularly to distributed healthcare. We prototype our usage enforcement engine in Java programming language with the support of Drools Expert as the policy evaluation engine. It is worth noting that Open Digital Right Language (with XML encoded) is used as the policy expression language in our experimentation.

REFERENCES

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

Ji-Won, B., Elisa, B., and Ninghui, L. (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.

Katt, B., Zhang, X., Breu, R., Hafner, M., and Seifert, J.-P. (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.

Li, W. and Hoang, D. (2009). A new security scheme for e-health system. In *Proceedings of the 2009 International Symposium on Collaborative Technologies and Systems*, pages 361–366, Washington, DC, USA. IEEE Computer Society.

Mohammad, J., Philip, F., Reihaneh, S.-N., Ken, B., and Paul, S. N. (2011). Towards defining semantic foundations for purpose-based privacy policies. In *Pro-*

ceedings of the first ACM conference on Data and application security and privacy, CODASPY '11, pages 213–224, New York, NY, USA. ACM.

Park, J. and Sandhu, R. (2004). The uconabc usage control model. *ACM Trans. Inf. Syst. Secur.*, 7:128–174.

Park, J. and Ravi, S. (2002). Towards usage control models: beyond traditional 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.

Rath, A. and Colin, J.-N. (2012a). Analogue attacks in e-health: Issues and solutions. CeHPSA - 2012 : 2nd IEEE International Workshop on Consumer eHealth Platforms, Services and Applications (CeHPSA)(accepted but unpublished).

Rath, A. and Colin, J.-N. (2012b). Patient privacy preservation: P-RBAC vs OrBAC in patient controlled records type of centralized healthcare information system. case study of walloon healthcare network, belgium. *The Fourth International Conference on eHealth, Telemedicine, and Social Medicine eTELEMED 2012*, 4:111–118.

Zhang, X., Parisi-Presicce, F., Sandhu, R., and Park, J. (2005). Formal model and policy specification of usage control. *ACM Trans. Inf. Syst. Secur.*, 8:351–387.