Protecting Personal Data: Access Control for Privacy Preserving Perimeter Protection System

Annanda Thavymony Rath, Jean-Noël Colin

Protecting Personal Data: Access Control for Privacy Preserving Perimeter Protection System*

Annanda Thavymony Rath and Jean-Noël Colin

Faculty of Computer Science, University of Namur, Belgium

Abstract. In this paper, we address the issues of personal data protection for privacy preserving perimeter protection system, particularly, the access control for real-time data streamed from surveillance tools and also for data stored in facility's storage. Furthermore, we also provide an access control model proposed specifically for such system and access control system implemented in Java.

Keywords: Access control, purpose enforcement, perimeter protection system, privacy-aware policies, access control system architecture.

1 Introduction

Critical buildings and infrastructures (e.g. nuclear power plants) require strong and unlikely breakable physical security protection from physical or forceful attacks. To protect such infrastructures beyond the use of conventional methods such as fences, we normally use different surveillance tools (e.g. visual cameras) to observe and detect activities around the protected infrastructures. In most cases, the surveillance covers only the private zones, but sometimes it goes beyond by covering a larger area (e.g. public area) in order to have an early warning, which provides enough time to react in case of attack. However, including the public area into the surveillance perimeter poses challenges for personal data protection since surveilling the public areas, without the approval from concern government authority, are not permitted in some countries like in EU or USA [4]. Thus, when designing perimeter protection system covering public area, one needs to take into account the personal data protection aspect [3][8]. We introduce, in this paper, an access control model and system designed particularly for P5 (Privacy Preserving Perimeter Protection Project) system [2]. The proposed access control system aims at ensuring that personal data are properly protected and only authorized people can use those data for purpose they intend for. The

* The work presented in this paper is supported by the European Commission's FP7 programme P5 Project (Grant agreement No: 312784). The content of this paper is the sole responsibility of the authors and it does not represent the opinion of the European Commission and the Commission is not responsible for any use that might be made of information contained herein.

rest of the paper is organized as follows. Section 2 is about P5 project and system architecture. Section 3 introduces the privacy-aware access control model. Section 4 presents the access control scenarios and policies definition for P5 system. Section 5 talks about access control architecture and implementation. Section 6 is related work and contributions while Section 7 is conclusion.

2 P5 Project and P5 System Architecture

P5 is the European and FP7 FUNDED (http://www.foi.se/p5) project for the protection of critical infrastructures to benefit the sustainability of society and future well-being of the European Citizens. The goal of the P5 project is an intelligent perimeter proactive surveillance system that works robustly under a wide range of weather and lighting conditions and that has strong privacy preserving features. In P5's system architecture (see Fig.1), there are many modules form-

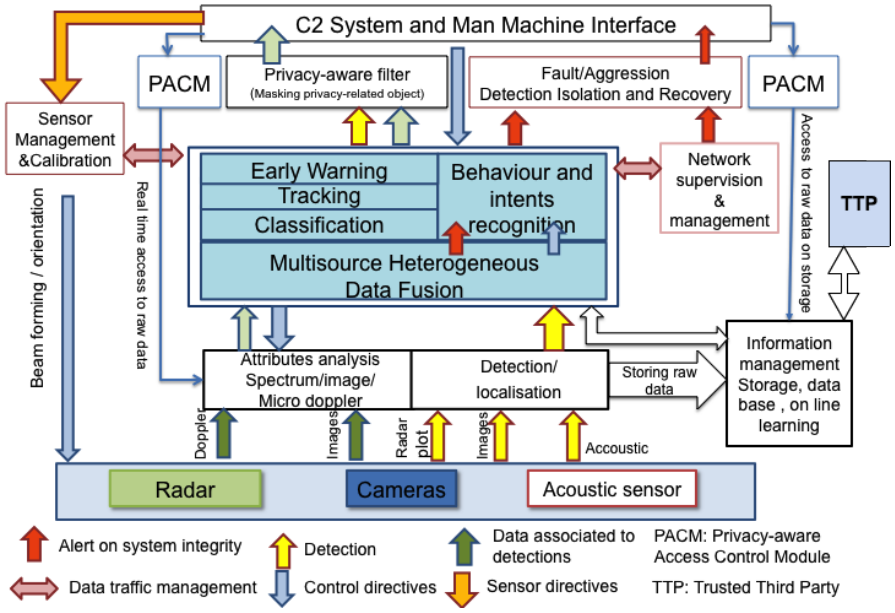

Fig. 1. Privacy preserving perimeter protection system architecture.

ing the entire P5 system, from the the lowest layer hosting sensors that provide different data types to the upper layer modules, such as "attributes analysis" , "detection/localization", "multi-source heterogeneous data fusion", "object classification, tracking and behavior and intents recognition", "early warning" and "man machine interface". Each one of the modules is a problem by itself, however, in this paper we address only the issue of access control for real-time data streamed from surveillance tools and data stored in facility's storage. There are

three modules, in the proposed architecture, which ensure privacy preservation and personal data protection: (1) Privacy-aware access control module (PACM) is responsible for controlling access to raw data. This module is responsible also for enforcing access control policies. (2) Privacy-aware filter is responsible for filtering the privacy-related information. (3) Trusted Third Party (TTP) module provides a way to manage access control policies, to protect the raw data and to audit the access to raw data. *TTP administrator* can be a trusted private or government entity, which is authorized for the job. It is important to note that since our main addressing issue in this paper is the design of privacy-aware access control system, we address only PACM.

3 Privacy-aware Access Control Model

Access Control Requirements. To identify the access control requirements for privacy preserving perimeter protection system, we conducted two different studies. Firstly, we worked with legal group to study the EU Directive 95/46/EC [4]. Secondly, we did a formal survey and also conducted a broad range of data collection and analysis. For the field works, we visited existing perimeter protection systems installed in the protected facilities in United Kingdom (UK) and Sweden, such as National Air Traffic control in UK and OKG Nuclear Power Plant in Sweden. Based on the result of our survey and legal studies, we can classify the access control and data protection requirements into four main points.

1. **Legal requirements:** based on the article 2, 10 and 11 of Directive 95/46/EC, we can define the following legal requirements. (1) Data controller needs to notify data subject every time of access. (2) Processing of private data is limited to the purpose for which data are intended for. (3) Consent from data subject is required when processing personal data.
2. **User management requirements:** security personnel manages access to control room as well as sensors. An assigned group of users, while they are on duty, is allowed to be in control room to view real time data streamed from sensors. In case of emergency where there are intruders attacking the facility, users in control room are allowed to access raw data. Other assigned group of users can access raw data in storage, but special access permission is needed. The main purpose of storing data from sensors is for forensic purpose.
3. **System performance requirements:** since we deal also with real-time data, access control to such data stream must be reasonably fast to avoid the delay to data stream.
4. **Security and data protection requirements:** processing of private data must be secured. We need to make sure that only authorized people can get access to data. Data controller should be a trusted entity that overlooks the management of access control policies as well as data in storage.

Based on the above requirements, we define the following access control model.

Access Control Model. We introduce Context- and Privacy-aware RBAC [3]

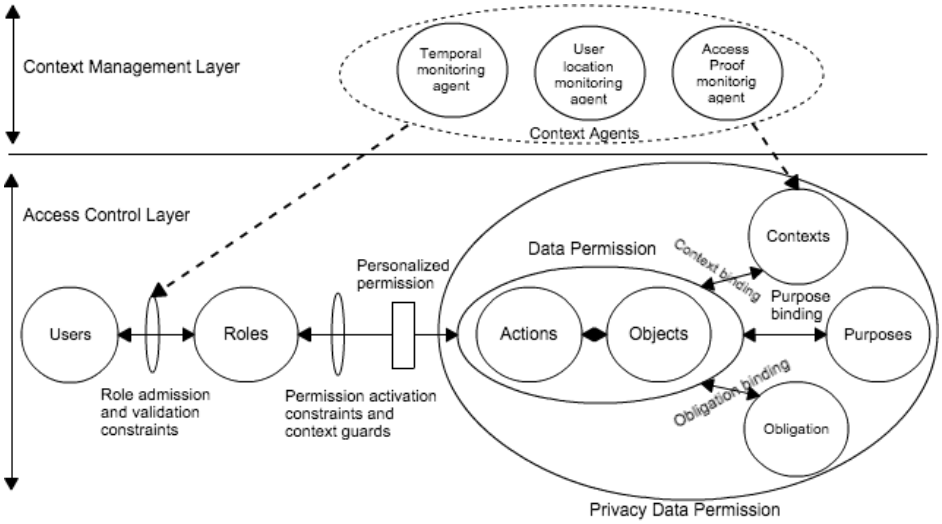

Fig. 2. Context- and Privacy-aware Role-Based Access Control Model (CP-RBAC).

(CP-RBAC), an access control model designed for controlling access to private data in privacy-preserving perimeter protection system. In CP-RBAC, access authorization is based not only on the user's role, but also on contextual information, such as temporal-, spatial- and environment-context. Furthermore, the concept of privacy is also introduced into the model. In the proposed model, contextual information is used as constraint for both the role admission and data permission assignment (see Fig. 2). The purpose of access and obligation are also the binding constraints on data permission to preserve and protect the privacy.

CP-RBAC (see Fig. 2) consists of the following entities.

- U is a set of users (u) where $u \in U$. R is a set of roles (r) where $r \in R$.
- A is a set of actions (a) where $a \in A$. D is a set of data where $d \in D$.
- P is a set of purposes (p) where $p \in P$. O is a set of obligations (o) where $o \in O$. C is a set of contextual variables (c) where $c \in C$.

Then, we formulate the privacy-sensitive policy (RP): $RP \subseteq R \times ((A \times D) \times (P \times C \times O))$. The detailed formulation of privacy-sensitive policy is as follows.

- The set of Data Permission $DP = \{(a, d) \mid a \in A, d \in D\}$
- The set of Privacy-sensitive Data Permission $PDP = \{(dp, p, c, o) \mid dp \in DP, p \in P, c \in C, o \in O\}$
- Privacy-sensitive Data Permission to role Assignment PDPA $\subseteq R \times PDP$, a many-to-many mapping privacy-sensitive data permission to role.

Contextual Data are the information surrounding user, data and reason that user needs to execute the action. Contextual information can be anything, such

as user's personal data, location or time.

Definition 1: Contextual variables expression

Let C be a set of contextual variables (c), where $c \in C$. "c" has the finite domain of possible values, denoted as DC where $dc \in DC$. "c" is equipped with the relational operators (Oprs) " $=, \neq, \geq, and \leq$ ". The condition of c has the form (c opr dc). Let c_1 and c_2 are two contextual variables in the form of the atomic condition. Then, $(c_1 \wedge c_2)$ or $(c_1 \vee c_2)$ is also condition.

Obligation is defined as the action that user or system needs to fulfill before or after accessing data. For example, notifying data controller every access.

Definition 2: Obligation expression

Let O be a set of obligation variables (o), where $o \in O$. "o" has the finite domain of possible values, denoted as B where $b \in B$. "o" is equipped with the relational operators (Oprs) " $=, \neq, \geq, and \leq$ ". The condition of "o" has the form (o opr b). For example, a payment obligation has the form: $payment \geq 50\$$.

---

4 Access Scenarios and Policy Definition for P5

We present the access scenarios and access control policies for P5. Then, we express those policies with the access control model we presented in Section 3.
1) Access Raw Data in Real Time (P1): we define the role "guardian" and users in this role are able to view real-time raw data streamed from sensors. However, they can do so only in case of emergency. Users can trigger emergency if and only if there is a positive acknowledgement from early warning module, which is responsible for providing a warning message when it detects an abnormal behavior of the objects. Moreover, to be able to keep track user's activities, users are required to notify system every time access to raw data. With above policy description, we are able to mine the following information.
- Role of user: "Guardian". Action: "View". Data: "streaming video".
- Context: "acknowledgement-from-early-warning".
- Purpose: "Observing-suspicious-object". Obligation: "notify".
With the above information and policy expression in Section 3, we can formulate the following access policy.

PDPA to role "Guardian" (P1)= (Guardian, (View, streaming video), Observing-suspicious-object, (acknowledgement-from-early-warning= positive), Notify=yes))

---

2) Replay Recent Past Raw Data (P2): this happens when guard in the control room wants to replay recent past video stream. We define "recent past video stream" as the video stream that has been recorded within the last 30 minutes

Users in role "guardian" are allowed to review recent past video stream. The same rule in P1 is applied in P2. However, one more context is required that is the life of video stream, which is set to be 30 minutes. The life of video stream context limits the access to the past videos, which are older than 30 minutes. Any access to older past video streams needs to be controlled by policy P3. With the above policy description, we are able to define the policy (P2) as follows.

PDPA to role "Guardian" (P2)= (Guardian, (View, streaming video), Observing-suspicious-object, (acknowledgement-from-early-warning= positive ∧ life-of-video ≤ 30 minutes), Notify=yes))

---

3) Access Raw Data in Storage (P3): authority may need to access past raw data for an investigation (e.g. a crime scene in the coverage area). However, in order to get access to raw data facility manager needs to send the request to TTP with proof. Proof is an official document justifying the mission. We define the role "Facility-security-manager" and users in this role are able to request TTP for accessing raw data in storage. In addition to that, users need to mention their purpose of request. We define three types of purpose: (1) Internal auditing, (2) Investigation and (3) Observing-suspicious-object. Moreover, to be able to keep track users' activities, users are required to notify system every access.
With above policy description, we are able to mine the following information.
- Role of user: "Facility-security-manager". Action: "View". Context: "proof".
- Data: "raw-video-in-storage". Purpose: "Investigation". Obligation: "notify".
With the above information, we can formulate P3 as follows.

PDPA to role "Facility-security-manager" (P3)= (Facility-security-manager, (View, raw-video-in-storage), Investigation, (proof= yes), Notify=yes))

---

5 Access Control: Architecture and Implementation

The access control system (see Figure 3) consists of the following components. Policy Enforcement Point (PEP) handles request from user and forwards it to PDP; PEP also enforces the policy by using different policy enforcement mechanisms: role to purpose alignment and notification. Policy Decision Point (PDP) is responsible for validating access control policies with the support of information provided by Policy Information Point (PIP). PIP is responsible for providing all needed information to PDP during policy validation phase. We define four contextual variables. (1) Proof is an official mission document that user needs to provide when requesting access to raw data in storage. (2) Early warning, this module is a part of P5's architecture (see Fig. 1). (3) User to role alignment provides information concerning the assignment of users to roles. (4) Working hours is the timetable of each user. We have implemented a context- and privacy-aware access control (CP-RBAC) system based on our proposed architecture (see Fig. 3) using Java. We have used XACML version 2 as the format for access control

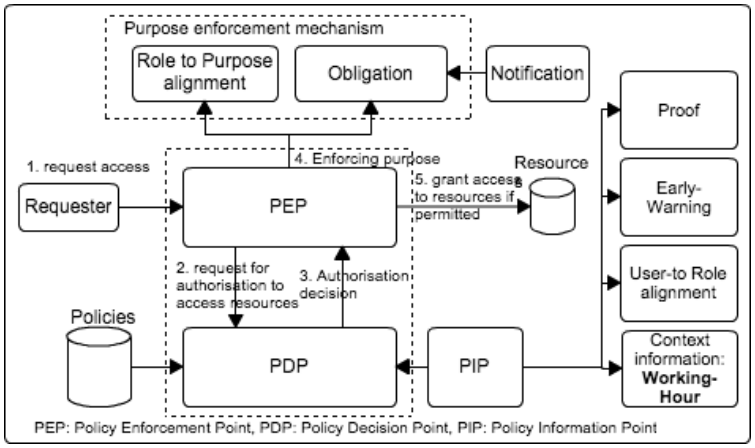

Fig. 3. Privacy-aware Access Control Architecture for P5 System.

requests, responses and policies [1]. We have also made use of Java Enterprise XACML library [1] as the policy decision point engine. We developed our program in Eclipse Standard/SDK (version Kepler) installed on Macbook air OS version 10.8.4, processor 1.3 Ghz Intel Core i5 with memory 8GB DDR3. We created 48 policies and expressed them with XACML policy language. The policies P1, P2 and P3 (see Section 4) are used as the models for the 48 policies. We performed six different tests with the same request structure, but different number of policies in the policy storages. There are two criteria we want to assess. The first criterion is the accuracy of the access control system we developed. This means it should provide 100% correct policy evaluation. The second criterion is the time required to evaluate a request. To evaluate second criteria, we created different access control policies with different level of complexity; then we find out the validation time for each request with different number of policies in storage. After several performance tests with the 6 different scenarios, we find that as the number of policies in storage increases, the time required to evaluate a request also increase; this is as expected. The first test scenario where there is only one policy in the policy storage, the time required to validate the policy is 344 milliseconds. With 48 policies, it takes 954 milliseconds.

6 Related Work and Contributions

After our thorough study of different access control models, we arrive to the conclusion of using RBAC [3] in P5 project, but with extension. We have also studied different models, such as DAC, MAC [3][5][6], ABAC [10] and OrBAC [9]. In context of P5 environment setting, most of access control models (like DAC and MAC) fail to respond to the requirements since such systems generally have

[1] https://code.google.com/p/enterprise-java-xacml/

very complex access control policies as we have illustrated in Section 3. P-RBAC [3] is another family of RBAC where the concept of privacy is introduced, but it does not address the contextual information. Moreover, it does not have the concepts of context-aware role admission and personalised role permission. With above reasons, we propose an access control model that takes into account the aspects like privacy [2][7]. To provide privacy preservation feature, the concept of purpose and obligation are introduced.

Contributions. Firstly, we propose the privacy preserving perimeter protection system architecture. Secondly, access control model that can be used to express privacy-aware access control policies in P5 system. The third contribution is the implementation of such access control system.

7 Conclusion

In this paper, we present a detailed architecture of privacy preserving perimeter protection system. We also present the context- and privacy-aware access control model that is designed specifically for such system. The access control system implemented in Java is also presented. Our future work is to focus on the development of TTP and the privacy-aware filter module.

References

1. Anderson, A. XACML profile for Role Based Access Control. http://www.oasis-open.org/committees/xacml (February 13 2004).
2. European Community Research And Development Information Service, 7 Framework Program. http://www.foi.se/p5, latest access: April 2014.
3. Ni.Qun, Bertino Elisa, Lobo Jorge, Brodie Carolyn, Clare- Marie Karat,Trombeta Alberto. Privacy-aware Role-Based Access Control. ACM Transaction Information and System Security (July 2010), 24:1-24:31.
4. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995. http://www.dataprotection.ie/ Latest access: December 2014.
5. D.F.Ferraiolo, R.Sandhu, S.Gavrila, D.R.Kuhn, R.Chandramouli. Proposed NIST Standard for Role-Based Access Control. In ACM Transactions on Information and System Security (August 2001), pp. 4(3):222-274.
6. Vincent C. Hu, David F. Ferraiolo, D. Rick Kuhn. Assessment of access control system. National Institute of Standards and Technology (September 2006).
7. C.A. Ardagna, M. Cremonini, S. De Capitani di Vimercati, P. Samarati. A Privacy-Aware Access Control System, in Journal of Computer Security (JCS), vol. 16, n. 4, September 2008, pp. 369-392.
8. Annanda Th. Rath, Jean-Noël Colin. Towards enforcement of purpose for privacy policy in distributed healthcare. The 3rd IEEE International Conference on Consumer eHealth Platforms, Services and Applications (CeHPSA), IEEE CCNC 2013.
9. FredeRic.Cuppens, And Nora.Cuppens. Modeling Contextual Security Policies in OrBAC. International Journal of Information Security (IJIS) 7, 4 (2008), 285-305.
10. Yuan, E., Tong, J. Attribute based access control a new access control approach for service oriented architectures (soa). Workshop, Ottawa, ON, Canada (April 2005).