A Secure RBAC Mobile Agent Model for Healthcare Institutions - Preliminary Study

Cátia Santos-Pereira[1], Alexandre B. Augusto[2], Ricardo Cruz-Correia[1,3], and Manuel E. Correia[2]

[1] Center for Research in Health Technologies and Information Systems - CINTESIS, Faculty of Medicine of University of Porto (FMUP) - Portugal
[2] Center for Research in Advanced Computing Systems - CRACS, Department of Computer Science, Faculty of Science of University of Porto - Portugal
[3] Department of Health Information and Decision Sciences - CIDES, FMUP
{catiap,rcorreia}@med.up.pt,
{aaugusto,mcc}@dcc.fc.up.pt

Abstract. Efficient healthcare is thus highly dependent on doctors being provided with access to patients medical information at the right time and place. However it frequently happens that critical pieces of pertinent information end up not being used because they are located in information systems that do not interoperate in a timely manner. There are many reasons that contribute to this grim state of affairs, but what interests us the most is the lack of enforceable security policies for systems interoperability and data exchange and the existence of many heterogeneous legacy systems that are almost impossible to directly include into any reasonable secure interoperable workflow. The objective of this paper is to establish a mobile agent access control model based on RBAC model that allows the exchange of clinical information between different health institutions that fall within the same circle of trust.

Keywords: Mobile agent, RBAC, HIS, Interoperability, Security.

1 Introduction

In this paper we propose a RBAC mobile agent access control model supported by a specially managed public key infrastructure for mobile agents authentication and access control. Our aim is to create the right means for doctors to be provided with timely accurate information, which would be otherwise inaccessible, by the means of strongly authenticated mobile agents capable of securely bridging otherwise isolated institutional eHealth domains and legacy applications [1].

2 Role Based Access Control Model

Our model follows the RBAC structure, where the role keeps the list of possible roles that an agent can assume. The permissions are linked to each different role where its operations are linked into each medical information object.

M. Bursa, S. Khuri, and M.E. Renda (Eds.): ITBAM 2013, LNCS 8060, pp. 108–111, 2013.
© Springer-Verlag Berlin Heidelberg 2013

The standard CEN/ISO 13606-4 [2] defines a set of functional roles and its mapping according to the record component sensitivity. Our proposed model takes advantage of this standard to perform the user-assignment and permission-assignment process. The attributes that mobile agent carries since its creation are used for the external institution agent to attribute a role and assign access permissions.

Furthermore our model includes the break the glass (BTG) mechanism [3] that is an important mechanism to mobile agents when an emergency scenario happens.

3 Mobile Agents: Creation and Migration Process

In order to create the right means to authenticate the mobile agents we had to establish a circle of trust between the health institutions. This circle was formed by the usage of a public key infrastructure (PKI) [4]. In this section we clarified the creation step and how an external should handle with it.

3.1 Mobile Agent Creation Process

The mobile agent creation have to two different steps: (1) the attribute gathering where the necessary attributes (see table 1) are collected in order to proceed the request; and (2) the request validation where the request is cryptographic signed in order to guarantee a non-repudiation between the involved entities.

3.2 Mobile Agent Reception Process

When a mobile agent arrives at an external health institution an external agent receives him by that verifies the mobile agent identity by the usage of the health institution signature attribute. After this process the external agent request the mobile agent cyphered symmetric key attribute in order to obtain the necessary symmetric key to decrypt the common attributes to define which permissions to grant to the mobile agent according to the access control model of the external health institution. Depending on the type of request the external access control could need an approval from an internal member of the institution in order to process the request. In cases like that the external agent provides to the mobile agent an identification number that could be used later to query the status of its requirement. This identification number improves the mobile agent flexibility since the mobile agent could keep his itinerary to other external health institutions and return later to consult the request status.

In special cases where the criticality code is set as emergency the mobile agent will active the BTG mechanism to directly obtain the requested medical information.

4 Case Scenario

To better understand how the agent access control model can be employed in real practice scenario, we exemplified a storyboard to serve as a keystone:

A 32 years old female patient named Inês, from Braga, 38 weeks pregnant, was admitted in the São João Hospital Centre, Emergency Department (ED) with severe abdominal pain. Due to the emergency situation she forgot her pregnancy book at home. Prenatal care was done in Braga Hospital. The doctor who assists the patient in ED, knowing that the prenatal care was done in Braga Hospital triggers an information request to Braga Hospital. He asks for blood analysis, obstetric history, previous pathologies and allergies.

The Figure 1 demonstrates the necessary steps since the agent is creation until the agent return. These steps are described as it follows:

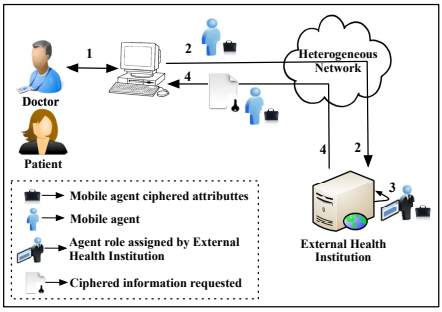

Fig. 1. Mobile agent messaging exchange

1. Doctor João logs into the HIS that recognizes his role (ED doctor). Then the doctor performs a clinical information request, if doctor João did not have enough permissions, the system would refuse the request. When doctor triggers this request in HIS a mobile agent is created and initiates its migration with a set of attributes presented in Table 1.
2. The user (Doctor João) logs into the HIS and the systems recognize his role (ED doctor) Then the doctor performs a clinical information request, if doctor João did not have enough permissions, the system would refuse the request. When doctor triggers this request in HIS a mobile agent is created and initiates its migration with a set of attributes presented in Table 1.
3. Mobile agent arrives to the external institution (Braga Hospital). The external agent authenticates the mobile agent by verifying the signatures attributes to ensure that its legitimate.
4. After perform authentication, the external institution RBAC module assign a role with access permissions. Since Doctor João is an emergency doctor in São João Hospital Centre and the reason appointed is care provision, the mobile agent will assume the Privileged healthcare professional role that can access almost all the patient information like demonstrated in Table 1. Since the authorization process succeeded, the mobile agent receives an authorization token to submit its query to the external agent.
5. Once finished, the mobile agent receives the results of the query and departs from external institution back to its home institution.

Table 1. Example of mobile agent non-ciphered attributes

Attribute	**Value**
User Id	43259823PRT
User role permission	ED doctor
Data query	([Blood analysis, obstetric history and allergies])
Patient id	PRT12343652
Criticality code	1
Time to response	7200000 milliseconds (2hours)
Reason code	01 (care provision)
List of external institution	([network host address, Braga Hospital certificate])
Description	38 weeks pregnant, admitted in São João Hospital Centre ED due to abdominal pain. Lacks pregnancy book.
Requester signature	ASd2qFHDFGg3g43g46G323sEa...We3
Health Institution signature	Juy7jgjT6rhgtg5SDFe3egt34FRd...DYJ

5 Conclusion

The consequence of unauthorized disclosure of health-related information may fatally affect a patients health, employment prospects and social standing. The main contribution of this work was to guarantee a secure communication channel between health institutions by the means of an access control for mobile agents.

This work is an initial proposal, the next steps are implementation and evaluation of our proposed model within a specific case study in a real healthcare institution, more precisely on São João Hospital Centre, which is the second biggest hospital in Portugal.

Acknowledgments. This work was financed through the project SAHIB [PTDC/EIA-EIA/105352/2008].

References

1. Vieira-Marques, P.M., Cruz-Correia, R.J., Robles, S., Cucurull, J., Navarro, G., Marti, R.: Secure integration of distributed medical data using mobile agents. IEEE Intelligent Systems 21(6), 47–54 (2006)
2. CEN/ISO 13606-4. Health informatics - electronic health record communication (2009)
3. Ferreira, A., Chadwick, D., Zao, G., Farinha, P., Correia, R., Chilro, R., Antunes, L.: How securely break into rbac: the btg-rbac model. In: Proceedings from 25th Annual Computer Security Applications Conference, ACSAC 2009 (2009)
4. Santos-Pereira, C., Augusto, A.B., Correia, M.E., Ferreira, A., Cruz-Correia, R.: A mobile based authorization mechanism for patient managed role based access control. In: Böhm, C., Khuri, S., Lhotská, L., Renda, M.E. (eds.) ITBAM 2012. LNCS, vol. 7451, pp. 54–68. Springer, Heidelberg (2012)