A secure RBAC mobile agent access control model for Healthcare Institutions

Cátia Santos-Pereira[1], Alexandre B. Augusto[2], Ricardo Cruz-Correia[3] and Manuel E. Correia[4]

[1,3]Center for Research in Health Technologies and Information Systems – CINTESIS, Faculty of Medicine of University of Porto (FMUP), Porto - Portugal
[2,4]Center for Research in Advanced Computing Systems (CRACS), Department of Computer Science, Faculty of Science, University of Porto, Porto - Portugal
[3]Department of Health Information and Decision Sciences (CIDES), FMUP - Portugal
{catiap[1], rcorreia[3]}@med.up.pt, {aaugusto[2], mcc[4]}@dcc.up.pt

Abstract

In medical organizations, healthcare providers need to have fast access to patients' medical information in order to make accurate diagnoses as well as to provide appropriate treatments. 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 inter-operate in a timely manner. Unfortunately the standard operational mode for many healthcare applications, and even healthcare institutions, is to be managed and operated as isolated islands that do not share information in an efficient 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 inter-operability and data exchange and the existence of many heterogeneous legacy systems that are almost impossible to directly include into any reasonable secure interoperable workflow.

In this paper we propose a RBAC mobile agent access control model supported by a specially managed public key infrastructure for mobile agent's strong 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.

Keywords: Mobile agent, Role-Based Access Control (RBAC), Health Information Systems (HIS), Interoperability, Information Security, Authentication.

1. Introduction

We are living in a fast paced highly mobile society with increasingly changing habits. As a result an ever greater number of patients end up taking medical treatments in distinct healthcare institutions all over a country, and even the world, during their lifetime. This process leaves a distributed trail of patients information scattered between very different institutions: analysis laboratories, primary care units, hospitals among others [1]. Therefore there is vast amount of clinical information about individuals that becomes deeply fragmented over a large number of distinct health information systems (HIS) [2] that usually have extreme difficulties in exchanging clinical information with each other and that for all practical purposes end up acting as isolated islands with important but unreachable clinical information.

In the healthcare domain, clinical information is normally collected into what is called the Electronic Health Record (EHR). The EHR encompasses many functions that can include different types of data items such as diagnoses, medications and operations that are responsible to feed health information systems (HIS). One of the main problems in HIS is the consistent lack of interoperability [3]. This is generally due to their complexity, heterogeneity and the constant concerns for data security [3, 4]. In order to address this interoperability problem, without doing major changes to legacy HIS, we propose a modular solution based on mobile multi-agents systems [5, 6] that acts as a portable and secure middleware to interconnect diverse heterogeneous HIS.

Mobile agent technology is having an ever-growing impact on the delivery of medical information [6]. They have proved to be very useful in the healthcare context for helping to solve interoperability issues that can arise when we try to connect different healthcare institutions [3]. They act in acquiring and manipulating information that resides in diverse information systems. A mobile agent is a particular class of agent with the ability to migrate to different locations over a network with a compatible agent platform carrying out specific tasks at the command of its creator-user [7]. Mobile agents offer

978-1-4799-1053-3/13/$31.00

many benefits in the healthcare environment. They are able to establish autonomous and asynchronous communications between different collaborating healthcare institutions. However the introduction of mobile agents creates some threats to the EHR since most of the EHR's data present a highly level of sensitiveness [8]. This requires a proper level of awareness in order to take the right countermeasures. The security and privacy issues that arise within this interoperability context can then be handled with the appropriate identity and authentication management, and access control mechanisms associated with secure cryptographic communication protocols [9]. In order to secure the patients' privacy the mobile agents must thus comply with the following properties:

- *Confidentiality*: Exchanged information cannot be accessible by unauthorized parties;
- *Integrity:* Exchanged information cannot be manipulated or modified during the information exchange without being detected;
- *Availability:* Information is accessible and available in a reasonable time when requested;
- *Non-repudiation:* Originating entity is responsible for its communications contents and cannot repudiate it.

Access control is the first barrier that a mobile agent finds when it tries to communicate with an external institution, since inadequate access control mechanisms carries some substantial risks as illustrated by the grim statistics observed during the year of 2012 by HIMSS [10]. In the USA over 1 million patients had their protected health information exposed during data breaches that occurred in healthcare organizations [11] by unauthorized accesses. However by applying well managed access control, health care institutions can ease the sharing of sensitive information between health information systems and at the same time reduce the number of data breaches incidents that can result from unauthorized accesses. Access control makes use of three different security processes *identification*, *authentication* and *authorization* of the respective entity. Identification is not a primarily security issue in itself, however the means by which an agent is identified are likely to affect the way a mobile agent can be authenticated. For example, a mobile agent could be identified by something like a serial number which is used only for the identifying process, or its identity could be associated with its origin and privileges by the usage of digital signatures that can be also used to authenticate the mobile agent by a digital signature verification process. Authentication is fundamental process for the establishment of a secure communications. Security related decisions cannot be solely made on the basis of a presentation of an agent identity. Moreover the authorization process happens when the external system checks if the agent can access the requested resources [12]. Therefore appropriate access control mechanisms are essential to provide a good balance between availability and confidentiality.

The most widely used access control model in healthcare is the Role Based Access Control (RBAC) [13, 14]. RBAC is considered particularly well suited for HIS since it provides several well-recognized advantages like simplicity and ease of administration, flexibility and scalability. This model assumes the concept that bases access control decisions on the functions the user is allowed to perform within an organization [13].

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 [15].

The paper is organized as follows: In section 2 we explain the mobile agent migration process giving the details of its creation. We also describe the main security aspects that were used to guarantee the agent authentication and the data confidentiality. In section 3 we described the RBAC and established a connection with the mobile agent by describing the respective formal descriptions and its roles and permissions. We also presented some mechanisms to improve the access control. In section 4 a case scenario was demonstrated describing each step in order to exchange medical information between health institutions. In Section 5, we derive our conclusions over the proposed model and set the next steps for future work.

2. 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). [16] In this section we described the necessary attributes and cryptographic means in order to create a mobile agent and how an external should handle with it.

2.1 Mobile agent creation process

When a user (e.g. healthcare professional) requests clinical information from an external health institution, an agent is created and sent to the external health institution. This agent carries several attributes in order to guarantee its identification at the external institutions. These attributes are gathered according to

the user role permissions in his healthcare institution access control model.

1. **User Id**: The user id is used to identify the person who is making the request. This id could be for example the identification number of the healthcare professional, which usually is a unique number plus the user's country code.
2. **User role permission**: Is a set of attributes used to inform an external institution the role and the permissions that the requester has in his health institution.
3. **Data Query**: This attribute is composed by a set of queries that requests the necessary medical information. The size of this set may varies according to the number of visiting health institutions. Each one of these queries is ciphered with a respective public key according to its health institution's destination.
4. **Patient Id:** This attribute is composed by a prefix and a suffix. The prefix holds the country code and the suffix contains the country patient's healthcare id in order to identify the patient in the multiple healthcare institutions.
5. **Criticality code**: The term criticality represents the emergency level of the request. This code is classified as 0 to non-emergency and 1 to emergency.
6. **Time to response**: This attribute is classified as a temporal attribute that is measured in milliseconds. Once this time expires the mobile agent returns to its home with the obtained results since requested medical information loses its value after expire date is reached.
7. **Reason Code**: A code number that represents the reason of the request composes this attribute. (E.g.: code 1 for care provision, code 2 for judicial purposes and so on.). This code list is shared between all the health institutions.
8. **List of external institutions**: This list is composed by a set of attributes that include: the visiting health institutions host addresses and their respective certificates.
9. **Description:** This is an optional open attribute. This attribute should be filled every time the requester considers that an additional justification is required.
10. **Requester signature:** This is an optional attribute depending on the health institution policies. If applicable, the requester by the usage of his health institution smartcard is required to sign all the previous attributes in order to establish a non-repudiation system.
11. **Health Institution signature**: The health institution validates the whole set of attributes by signing it. This signature is essential for the mobile agent since external healthcare institutions only accept signed mobile agent that falls in their circle of trust.

After gather these attributes, the mobile agent initiate its migration by the usage of the List of external health institutions.

2.2 Agent reception process

When a mobile agent arrives at an external health institution a 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 attributes in order 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 1 (emergency) and an internal member approval is needed the external agent will active a special mechanism known as Break the Glass (BTG) to directly obtain the requested medical information. The BTG mechanism is already described in subsection 3.3.

3. Role Based Access Control Model

The National Institute of Standards and Technology (NIST) proposed the Role Based Access Control model [13] including the Core RBAC and later the Hierarchical RBAC and the Constrained RBAC (which includes Separation of Duties (SoD). In this section we defined a formal description of an agent access control model based on RBAC and explained how assigned access permissions to a mobile agent in an external institution.

3.1 Formal description

Figure 1 presents the elements and their relations in the RBAC model using agents. "User Agent" is the same as a "User" of the original RBAC model.

In our model, Role keeps the list of roles that an agent can assume. Permissions, keep the list of

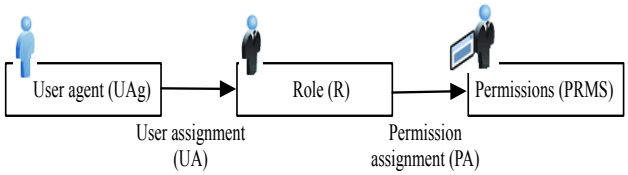

Figure 1: Elements and their relations in the Core RBAC model using agents.

permissions that an agent role can assume. Permissions are composed of operations (OPS) applied to objects (OBS). An agent will have access to a certain OBS if it has any OPS available (e.g. create, read, update, delete or execute) [17].

UAg - a set of agents, R - a set of roles, PRMS - a set of permissions, OPS - a set of operations, OBS - a set of objects.

a) *UA ⊆ UAg x R, a many-to-many mapping between user agents onto a set of agent roles (user-to-role assignment relation).*
b) *RH ⊆ R x R, partially ordered role hierarchy (RH)*
c) *PRMS ⊆ R x PRMS, a many-to-many mapping between agents role onto a set of agents permissions (role-to-permission assignment relation).*

The access control permissions includes only read operation [17]. These operations are linked to each different role into each medical information document. When a mobile agent assumes a role assigned by the external institution he has permissions only to read and execute.

3.2 Roles and permissions

The CEN/ISO 13606-4 [18] defines a set of clinical information classification with a sensitivity value scale (1 less sensitive to 5 more sensitive) that an EHR may integrate (*personal care*, *privileged care*, *clinical care*, *clinical management* and *care management*). For example, a clinical information can be classified as personal care that corresponds to a sensitivity value of 5 if the sensitivity of this information justifies that only be shared by the subject of care (patient) perhaps with only one or two people whom they trust most. On the other hand if the information is less sensitive it can be classified as care management that corresponds to sensitivity value of 1 and can be accessed by administrative staff for instance.

This standard also describes a set of functional roles such as:

- *Subject of care* (usually the patient);
- *Subject of care agent* (e.g. parent, guardian...);
- *Personal healthcare professional* (healthcare professional with the closest relationship to the patient, e.g. GP);
- *Privileged healthcare professional* (nominated by the healthcare facility of care, if there is a nomination such as an emergency over-ride);
- *Healthcare professional* (party involved in providing direct care to the patient);
- *Health-related professional* (party indirectly involved in patient care, teaching, research etc);
- *Administrative* (others parties supporting service provision to the patient).

Table 1: Mapping of functional roles in clinical information according with a sensitivity scale. Adapted from [18].

	Clinical information sensivity classification				
Functional Role	**Care management**	**Clinical management**	**Clinical care**	**Privileged care**	**Personal care**
Subject of care	Y	Y	Y	Y	Y
Subject of care agent	Y	Y	Y	Y	Y
Personal healthcare professional	Y	Y	Y	Y	Y
Privileged healthcare professional	Y	Y	Y	Y+	++
Healthcare professional	Y	Y	Y	N	N
Health-related professional	Y	Y	N	N	N
Administrative	Y	N	N	N	N

NOTE 1 Y indicates that access will be granted to Clinical information of this sensitivity unless otherwise dictated by other policy constraints, as specified according to clause 7 of this part standard.
NOTE 2 Y + Indicates that access will be granted if the EHR Recipient is a member of the same specialty or clinical service as that in which the Record _Component was created e.g. sexual health clinic, prison health service (as specified in the service_setting attribute for the composer of the Composition in the Reference Model of Part 1). This access may also be granted in health care emergency situations if so authorized.
NOTE 3 ++ Indicates that access to Personal Care information may sometimes be granted by mandate to Privileged Healthcare Professionals in some care settings, such as in the armed forces of some countries.

Table 1 shows the mapping of functional roles in record components sensitivity. The proposed authorization model uses this schema to perform the user-assignment and permission-assignment process. The attributes that mobile agent carries since his creation are used for the external institution agent to attribute a role and assign access permissions.

3.3 Break the glass access

The BTG mechanism is used to break or override the access controls in a controlled manner. In other words this should allow a user to override the access control rules stated by the access control manager and access what he requests, even thought he was not previously authorized to do it. When this is done, BTG rules come into play reporting the user's actions, thus making him responsible for his requests and oblige him to justify the request [19].

This is an important mechanism to mobile agents when an emergency scenario happens. For example when a mobile agent is in an external health institution and does not have enough permission to access crucial medical information that a healthcare professional needs to save a patient.

The break the glass also works as a non-repudiation mechanism since the requester is strongly audited after decided to proceed with the BTG and all involved parties are notified.

3.4 Audit

Access control is not a complete solution for securing a system. It must be coupled with auditing. Audit controls concern a *posteriori* analysis of all the requests and activities of users in a system, this process ensure that authorized users do not misuse their privileges [20]. Extensive auditing is important to ensure traceability of user actions, in this case in mobile agent actions.

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.* "

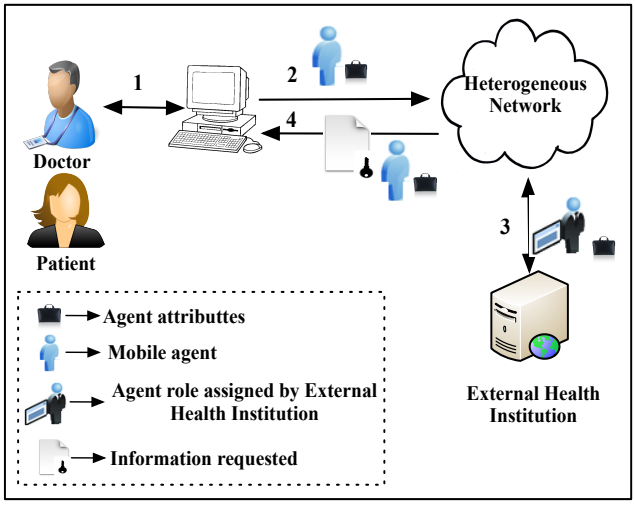

Figure 2: Mobile agent access control model messaging exchange.

The **Figure 2** demonstrates the necessary steps since the agent is creation until the agent return.

Step 1 - 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 2**.

Step 2 - Mobile agent arrives to the external institution (Braga Hospital). The external agent authenticates the mobile agent by verifying the signatures attributes to ensure that it's legitimate.

Step 3 - 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 2**. Since the authorization process succeeded, the mobile agent receives an authorization token to submit its query to the external agent.

Step 4 - Once finished, the mobile agent receives the results of the query and departs from external institution back to its home institution.

5. Conclusion and future work

The consequence of unauthorized disclosure of health-related information may fatally affect a patient's

Table 2: Example of mobile agent non-ciphered attributes

User id	43259823PRT
User role permission	ED doctor
Data query	(Blood analysis, obstetric history, previous pathologies 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	Patient, 38 weeks pregnant was admitted in São João Hospital Centre ED due to abdominal pain. Lacks pregnancy book.
Requester signature	ASd2qFHDFGg3g43g46G32d4g... EFD
Health Institution signature	Juy7jgjT6rhgtg5SDFe3egt34FRd... DYJ

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 a strong 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.

Acknowledges

This work is funded by FEDER funds (Programa Operacional Factores de Competitividade – COMPETE) and by National funds (FCT – Fundação para a Ciência e a Tecnologia) through project SAHIB - Enhancing multi-institutional health data availability through multi-agent systems [PTDC/EIA-EIA/105352/2008] and project OFELIA - Open Federated Environments Leveraging Identity and Authorization [PTDC/EIA- EIA/104328/2008].

References

[1] P. M. Vieira-Marques, R. J. Cruz-Correia, S. Robles, J. Cucurull, G. Navarro, and R. Marti, "Secure integration of distributed medical data using mobile agents," Ieee Intelligent Systems, vol. 21, pp. 47-54, Nov-Dec 2006.

[2] S. K. Katsikas, "Health care management and information systems security: awareness, training or education?," *Int J Med Inform,* vol. 60, pp. 129-35, Nov 2000.

[3] R. Cruz-Correia, P. Vieira-Marques, P. Costa, A. Ferreira, E. Oliveira-Palhares, F. Araujo, and A. Costa-Pereira, "Integration of hospital data using agent technologies - A case study," *Ai Communications,* vol. 18, pp. 191-200, 2005.

[4] R. A. Martins, M. E. Correia, and A. B. Augusto, "A literature review of security mechanisms employed by mobile agents."

[5] T. L. Chen, Y. F. Chung, and F. Y. S. Lin, "A Study on Agent-Based Secure Scheme for Electronic Medical Record System," *Journal of Medical Systems,* vol. 36, pp. 1345-1357, Jun 2012.

[6] M. Nikooghadam and A. Zakerolhosseini, "Secure Communication of Medical Information Using Mobile Agents," *Journal of Medical Systems,* vol. 36, pp. 3839-3850, Dec 2012.

[7] W. Jansen; and T. Karygiannis, "NIST Special Publication 800-19 Mobile Agent Security," 2000.

[8] K. Hayrinen, K. Saranto, and P. Nykanen, "Definition, structure, content, use and impacts of electronic health records: A review of the research literature," *International Journal of Medical Informatics,* vol. 77, pp. 291-304, May 2008.

[9] N. Borselius, "Mobile agent security," *Electronics Communication Engineering Journal,* vol. 14, pp. 211 - 218, 2002.

[10] HIMSS. (2012). *HIMSS.* Available: http://www.himss.org/ASP/index.asp

[11] H. Analitics;, "Security of patient data," USAApril 2012 2012.

[12] *Health Informatics - Privilege management and access control* ISO/TS 22600-2:2006, 2006.

[13] R. Sandhu, D. Ferraiolo, and R. Kuhn, "The NIST model for role-based access control: towards a unified standard," presented at the Proceedings of the fifth ACM workshop on Role-based access control, Berlin, Germany, 2000.

[14] A. Ferreira, R. Cruz-Correia, L. Antunes, and D. Chadwick, "Access control: how can it improve patients' healthcare?," *Stud Health Technol Inform,* vol. 127, pp. 65-76, 2007.

[15] G.-J. Ahn and J. Lam, "Managing privacy preferences for federated identity management," presented at the Workshop on Digital identity management, Fairfax, VA, USA, 2005.

[16] B. Schneier, *Applied cryptography (2nd ed.): protocols, algorithms, and source code in C*. New York, NY, USA: John Wiley \& Sons, Inc, 1995.

[17] The Internet Society, "Security Audit and Access Accountability Message XML Data Definitions for Healthcare Applications," vol. RFC 3881 ed, 2004.

[18] *Health informatics - Electronic health record communication* ISO/TS 13606-4:2009, 2009.

[19] A. Ferreira, D. Chadwick, G. Zao, P. Farinha, R. Correia, R. Chilro, and L. Antunes, "How securely break into RBAC: the BTG-RBAC model," *Proceedings from 25th Annual Computer Security Applications Conference - ACSAC 2009,* 2009.

[20] R. S. Sandhu and P. Samarati, "Access-Control - Principles and Practice," *Ieee Communications Magazine,* vol. 32, pp. 40-48, Sep 1994.