# Pervasive secure electronic healthcare records management

Petros Belsis[1], Apostolos Malatras[2] Stefanos Gritzalis[1] Christos Skourlas[3], Ioannis Chalaris[3]

[1]Department of Information and Comnmunication Systems Engineering, University of the Aegean, Karlovasi, Samos, Greece
[2]Department of Electronic Engineering, Centre for Communications Systems Research, University of Surrey, UK
[3]Department of Informatics, Technological Education Institute, Athens, Greece

**Abstract.** Pervasive environments introduce a technological paradigm shift, giving a new impetus to the functionality of applications, overcoming applicability barriers of legacy applications. Electronic healthcare records management can clearly benefit from the new challenges brought by this emerging technology, due to its low cost and high percentage of user adoption. Still, the sensitivity of medical data, poses new requirements in the design of a secure infrastructure based on the ad-hoc networking schema, which underlies pervasive environments. User authorization and controlled access to information is of outmost importance. This paper proposes a management system for electronic healthcare records satisfying the aforementioned security requirements.

## 1 Introduction

The rapid establishment of wireless technologies and their applicability to a wide range and of various requirements environments, enables – among others – medical domains with extended functionalities, providing their users with information accessible at any time and independently of location within their range. The continuous growth in the use of mobile devices and their relatively low cost causes a shift from traditional applications and stable networking infrastructures, to the one based in Mobile ad-hoc networks and other ubiquitous communications enablers. These networks, pose new security challenges to electronic healthcare records domain, due to the sensitivity of the data transmitted over insecure, wireless links; as well as due to the instability of the infrastructure, which consists of several temporary participating nodes. A major concern is brought by the mere notion of access to everyone, everywhere that pervasive systems employ, as this contradicts every well-known security principle.

Pervasive infrastructures are relying upon the concept of mobile ad-hoc networks (MANETs) [1]. This can be considered as a serious drawback due to the versatility of nodes. Therefore, MANETs should not be adopted as a universally acceptable

Belsis P., Malatras A., Gritzalis S., Skourlas C. and Chalaris I. (2005).
Pervasive secure electronic healthcare records management.
In *Proceedings of the 2nd International Workshop on Ubiquitous Computing*, pages 101-110
DOI: 10.5220/0002572801010110

solution for every networking problem. Node mobility can lead to network instability, and requires the adoption of pioneering solutions and innovative design in both the underlying protocols as well as the supporting infrastructure.

IT enabled healthcare support on the other hand, raises constant demands for the establishment of high quality services, accessible anywhere within a medical department, leading thus to a utilization of mobile infrastructures. Though many enterprise solutions exist for wireless applications they confront to conventional security mechanisms [2], which fail to meet the extensive requirements of ubiquitous environments. This dynamic environment imposes several additional security requirements mainly related to the access control mechanisms for the sensitive, private healthcare records information.

We are addressing the problem of providing transparent access to patient's records within a distributed coalition among medical domains. We discuss the notions encompassing issues relative to the secure provision of transparent access to text resources (medical files), according to a policy based management framework. In order to prove the validity of our assumptions, we argue about a set of implementation choices incorporated through our prototype, the functionality of which and scalability potential is continuously rising.

The rest of this paper is organized as follows: Section 2 discusses related work and motivations for our work. Section 3 provides our requirements analysis for the proposed system design architecture; section 4 discusses our policy based management framework, while section 5 provides implementation details and an evaluation framework. Section 6 concludes the paper, providing directions for future and ongoing work.

## 2 Related work

### 2.1 Health records management

Electronic health records management attracts significant international interest [3] and sets the scenery for the establishment of a distributed, coalition-based, security policy enhanced records exchange framework among different medical domains. Several European projects have proposed candidate solutions for secure inter-operations between medical domains [4]. In the HARP project, security profiles related with access rights are dynamically downloaded to the client side. The MEDITRAV EU-project attempts to overcome national or linguistic barriers by adopting the solution of a multilingual portable personal record. Security implications of medical records treatment are discussed in [5] [6]. These approaches, pose mainly their research effort on the security requirements for effective electronic health record management, still they confront mainly to stable infrastructures; on the other hand, requirements necessary for the dynamic nature and diverse characteristics of versatile mobile ad-hoc networks are totally neglected. In [2] pervasive patient record management is discussed, yet authentication schemes are based on a totally different model, this of decentralized trust management [7]

### 2.2 Wireless healthcare applications

Wireless mediCenter [8], is a system for management of electronic medical records and delivery through secure LANs or high-speed wireless connections. It provides different portals for doctors and patients in order to achieve classification of access permissions. It does not provide a flexible secure management framework for cooperating medical domains, while its scalability potential is considerably low. The m-Care project [9], aims at providing secure access through a WAP based architecture. Users and access rights related information is kept in an MS-SQL Server database. As its security model is based on simple access control lists its flexibility and efficiency concerning to maintaining access rights related information is seriously questioned.

## 3 Design choices

### 3.1 Requirements analysis

Effective design and implementation of pervasive health care applications should be driven by a number of requirements, related mainly with the sensitive nature of patient's medical records data content. These requirements are mostly dictated by the mere nature of the communications paradigm we have adopted, that of pervasive technologies. In order to handle these issues from both a technical perspective as well as for compliance purposes with the legislative principles enforced by EU directives relative to sensitive data protection, we adopted a number of implementation choices in our project, covering various issues, not treated so far by other similar approaches. Such issues are:

- Policy driven approach. We argue that policy driven approach is more suitable for medical environments, since the trust based model maps unknown roles to users and therefore assigns privileges to them accordingly to the reputation collected for them for other models. We believe that this model is suitable for environments characterized by total adhocracy and absence of well stated organizational policy, still it cannot be applied to well policy configured, medical environments.
- Concern about the limited resources in terms of processing power, memory or energy supplies. The presence of devices with sufficient resources should not be considered the rule, but rather the exception.
- Agent based discovery and authentication. In order to perform a patient's related record identification among a number of domains in a distributed environment, we utilize software agents, which through the means of a predefined ontology they communicate and collect information on the user's behalf.

### 3.2 System Architecture

The need to create a pervasive environment based on transparent and secure dissemination of health records among authorized users is the driving force behind our framework. In a traditional stable networking infrastructure, access to medical records -presuming a policy based approach- can be materialized through a single policy interpretation and decision point, where a user performs a request to log on to a certain service and security considerations are handled within the service's framework, providing therefore access only to users having the necessary level of clearance. This centralized policy interpretation approach is totally inapplicable to our environment, where instability is a main characteristic. Furthermore, providing a similar architecture based on nodes with reduced reliability can direct to the provision of a single point of failure. Due to the absence of stable links, there is a wireless interconnection of all the devices, therefore providing access to all edges of the virtual network. Our approach builds upon utilizing a hybrid set of both stable devices and mobile devices. The focal points of the system, where role and policy repositories reside and authentication occurs are supported by redundant identical entities to ensure continuous and uninterrupted operation. In addition, the selection of the devices to host these services occurs not in a random manner, rather by taking into account the device relative stability in the volatile network topology.
Through the provision of user agents, implemented in the JADE platform [11], and by means of a predefined ontology developed on Protégé [12] ontology editing tool, we automate the medical records identification procedure. The usage of ontology is a prerequisite in order to standardize the terminology concepts exchanged between the agents. Table 1a provides a sample of an Agent Communication Language (ACL) message exchange based on our role hierarchy ontology for the medical domain. Table 1b defines an ACL message according to the FIPA-query protocol [13], expressing the validity of the previous role assignment hierarchy.

**Table 1a** (left). Expression of an SL type definition of role hierarchy presenting that Doctor and nurse in oncologist clinic have different hierarchy –and therefore permissions classification. **Table 1b** (right). Example of ACL message based on the previous ontology according to the FIPA-query- agent interaction protocol.

| | |
|---|---|
| (ANCESTOROF<br>:source (ROLE<br>:name oncologist<br>:definedBy (DOMAIN<br>:name OncologyDept))<br>:target (ROLE<br>:name nurse<br>:definedBy (DOMAIN<br>:name OncologyDept)) | (inform<br>:sender (agent-identifier :name agentA)<br>:receiver (set (agent-identifier :name agentB))<br>:ontology auth-ontology<br>:language fipa-sl0<br>:protocol fipa-query<br>:content<br>"(ANCESTOROF<br>:source (ROLE<br>:name doctor<br>:definedBy (DOMAIN :name OncologyDept))<br>:target (ROLE :name nurse<br>:definedBy (DOMAIN :name OncologyDept))")) |

Several considerations needed to be taken due to the instability of the wireless connections. Mainly we confront to security concerns, ensuring there will be no breach in confidentiality of medical records. In order to retain the scalability potential and support for large number of roles, we confront to the Role Based Access Control (RBAC) [18] framework. The storage of access control information especially on distributed environments where the number of assets to be managed grows progressively - as well as the number of users- and cannot be efficiently managed through the usage of contemporary authentication and access control schemes, such as Access Control Lists (ACL's). The usage of policies and policy languages can simplify the management of distributed systems, which contain of large number of objects which often span across organizational boundaries [19]. We adopted in our approach the eXtensible Access Control Markup Language (XACML) [10], through which we achieve platform independency and support interoperability characteristics of the system in its entity; XACML can be codified in eXtensible Markup Language (XML) which is specially designed to perform as interoperable data codification format, suitable for integration to several platforms, such as Web Services and other Web based environments.

## 4 Access control decisions on distributed health environment

Due to the dynamic nature and the presence of different roles from several medical domains (i.e. hospitals) we have to ensure prior to a record distribution that the proper access rights are maintained by a specific role requesting access to a resource. A suitable management framework is that of the XML based XACML access control language. This model in general operates as depicted in Fig 1.

The administrator is editing the policy and makes it available to the Policy Decision Point (PDP). When a request is made, it is directed to the Policy Enforcement Point (PEP). Now the PEP directs the request to the PDP which prior to inspecting the request's compliance with the predefined policy, requests additional context information from the Context Handler. Accordingly the PDP authorizes or not the requester and provides access to the service. Several security considerations arise when it comes to the applicability of this scheme to our framework. First, in a single domain environment there is a well-defined role and associations upon them, hierarchy. This is inapplicable here, where several participating domains with different role hierarchies, different roles and permissions are involving. In order to enable this cooperation scheme therefore we adopted the following solution. Each domain has its well-defined policy based on the grounds of the policy language. We create a global role hierarchy scheme, and prior to different domain participation, the administrators have to pre-establish a role mapping of the joining organization to the global hierarchy scheme. Administrators are aware of the ethical and legal implications of an incorrect role assignment, as well as they are aware of the policy language specifications in order to perform role assignment.

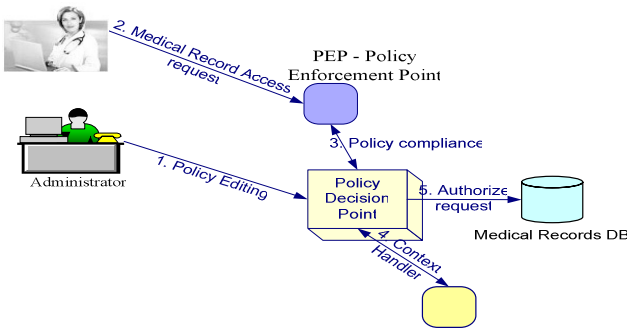


**Fig. 1.** XACML access control framework overview

This mapping is not enough though, due to the topology of the network, which cannot be based on a single policy enforcement and decision point. Therefore, we consider several nodes to play the role of PEPs and PDPs employing well established and documented techniques of redundancy proposed for the unstable pervasive environment. Each node that provides direct access to medical records has to be able to enforce policy decisions [Fig 2] to control access to this information.

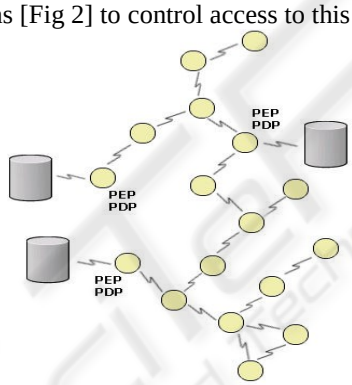


**Fig. 2.** Adjustment of XACML model to pervasive infrastructures

## 5 Implementation details

In order to test the validity of our framework, we experimented with a set of 4 laptops (INTEL Centrino's and Mobile Celeron's) containing wireless cards, which played the role of the mobile nodes. We implemented different role hierarchies for three medical domains, edited on Protégé ontology development kit. We used as an example an oncology clinic, a cardiology clinic and a general clinic. For each clinic we implemented the WardManager role, the doctor role (oncologist, cardiologist) a nurse role and a patients role. We presume that the general clinic role hierarchy functions as the federal role hierarchy, to which the other domains have to confront. For patients we created a simple historic record, consisting of their name and lab test results, recorded in XML format (Fig. 4).

Patients and nurses were defined to view only personal details; doctors and wards were authorized to view lab tests also. We considered all nodes to contain several medical records. XACML enables context-based authorization, based on the domain. By forming an appropriate XACML request message, the PDP was able to define whether the specific user was authorized or not, by identifying his role and the domain he belongs to (defined as part of his personal data). Our framework is dealing with high-level security considerations in pervasive environments. We used standard encryption schemes (WEP) for the lower communication levels, in order to avoid eavesdropping or identity tampering.

The Java platform, J2SE 1.4, was the basis of our implementation due to the need for interoperability amongst the variety of platforms that can be found in pervasive environments. Another reason was the immediate integration with the JADE agent platform that forms the basis of our proposed approach. We understand that the Standard Edition of the Java Runtime that we used is processing demanding for small mobile devices, but we consider switching to J2ME when testing with such devices in the future. The Apache Xerces2 XML Parser handles XML processing, since it widely adopted and viewed as the baseline solution to Java-based XML parsing. Moreover and in accordance to the previous statement, lightweight XML processing in the future will be handled by the kXML2 Parser, which is targeted to small devices with limited resources and is J2ME compliant.

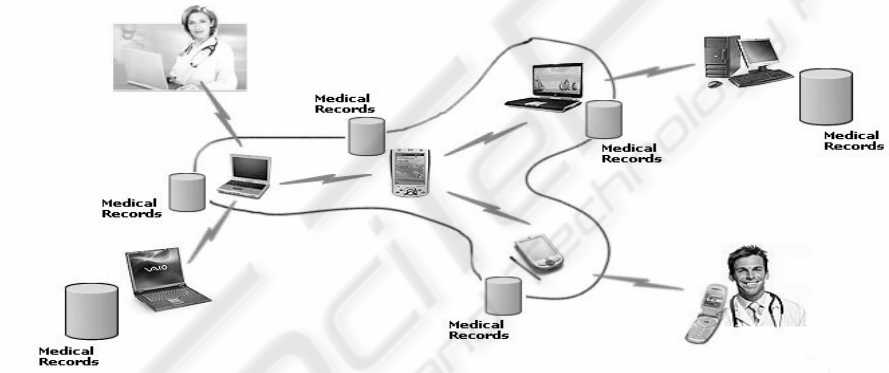


**Fig. 3.** Overview of pervasive health records management framework.

## 6 Conclusions

Security is a major issue in medical environments. Electronic patient record's management poses new challenges when it comes to its applicability to pervasive environments. Such a framework can prove to be beneficial to all roles related with such an environment, including doctors, nurses, and patients. In a real life scenario, the doctor can acquire at anytime and any place within the range of a hospital, information relative to patient's medical history, previous treatments or medication, by simply using his mobile device (Fig. 3) (enabled with 802.11b, Infrared, or Bluetooth communication capability).

Pervasive environments are built upon mobile ad-hoc networks. Adaptations and extensions [14] of classical topology-based routing protocols known from static networks are coping with the problem of permanent link failures due to device mobility. Furthermore, except form this adaptation to network protocols design, due to their unstable architecture, they demand a totally innovative design of their security management scheme. The large number of users and roles coming from different domains requires further considerations concerning the deployment and enforcement of security decisions. Our approach is policy-based, confronting with the RBAC access control model. Additively, we provided a flexible solution for the multi-domain role equipollence problem and we redesigned the XACML policy enforcement scheme in order to become applicable to pervasive environments. We adjusted the standardized XACML based authorization scheme to a distributed architecture, suitable for the instability issues that characterize MANET's infrastructures.

Another characteristic of our approach is the transparency it provides, based on the utilization of software agents. The agents were implemented in the JADE platform, and were used for identification of medical records related to a specific patient, as well as for performing authorization procedures transparently to the user, by providing to the PDP the user's credentials. This transparent identification and authorization scheme, utilized concepts described in [15]. We plan to expand our experimentation by utilizing protocols such as these described in [16] [17], and to apply the scenario on a more complex hardware infrastructure.

## Acknowledgments

The authors would like to thank John Varnas for providing assistance with the drawings. We would also like to thank the anonymous reviewers for their insightful comments.
This work was co-funded by 75% from E.E. and 25% from the Greek Government under the framework of the Education and Initial Vocational Training Program – Archimedes.

## References

1. Perkins, C. E., Ad Hoc Networking, 2001 Addison Wesley Longman Inc.
2. A. Choudhri, L. Kagal, A. Joshi, T. Finin, and Y. Yesha, "PatientService : Electronic Patient Record Redaction and Delivery in Pervasive Environments", Fifth International Workshop on Enterprise Networking and Computing in Healthcare Industry (Healthcom 2003), Santa Monica, June 2003
3. Scott R.E., Jennet P., Yeo M. Access and authorization in a Global e-Health Policy context. International Journal of Medical Informatics (2004) 73, 259-266.
4. Ruotsalainen P. "A cross platform model for secure Electronic health record communication", International Journal of Medical Informatics, (2004) 73, 291-295
5. Kokolakis, S., Gritzalis, D. and Katsikas, S. (1998a). Generic security policies for healthcare information systems. *Health informatics journal*, 4(4), 184-195.

6. Katsikas, S. and Gritzalis, D. (1996). High level security policy guidelines. In The SEISMED Consortium (eds), *Data security for health care*. IOS Press, Amsterdam.
7. M. Blaze, J. Feigenbaum, J. Ioannidis, and A. Keromytis. The keynote trust management system version. Internet RFC 2704, September 1999
8. Wireless Medicenter. http://www.wirelessmedicenter.com/mc/glance.cfm
9. David Brazier, Alpha Bravo Charlie Ltd. The m-care project. http://www.m-care.co.uk/tech.html
10. Organization for the Advancement of Structured Information Standards (OASIS), ''XACML Extensible access control markup language specification 2.0'', OASIS Standard, (available at http://www.oasis-open.org
11. The JADE agent development kit. Available at http://jade.tilab.com/
12. Protégé ontology development kit. http://protege.stanford.edu, (2004)
13. FIPA Standard Status Specifications. www.fipa.org/repository/standardspecs.html
14. Elizabeth M. Royer and Chai-Keong Toh. A review of current routing protocols for ad-hoc mobile wireless networks. *IEEE Personal Communications*, pages 46.55, April 1999.
15. Belsis P., Gritzalis S., ''Distributed autonomous Knowledge Acquisition and Dissemination ontology based framework'', Proceedings of "Interop" Workshop on Interoperability, H. Kuehn ed., November 2004, Vienna, Austria, pp. 100-104
16. R. Friedman, M. Gradinariu and G. Simon, "Locating cache proxies in MANETs", ACM MobiHoc 2004
17. P.-J. Wan, K. M. Alzoubi and O. Frieder, "Distributed construction of connected dominating set in wireless ad hoc networks", IEEE Infocom 2002
18. Ravi Sandhu, David Ferraiolo, and Richard Kuhn. The NIST model for role-based access control: towards a unified standard. In Proceedings of the Fifth ACM Workshop on Role-Based Access Control (RBAC'00), pages 47–63, 2000.
19. Damianou, N., N. Dulay, E. Lupu and M. Sloman . Managing Security in Object-based Distributed Systems using Ponder. In Proceedings of the 6th Open European Summer School (Eunice 2000), Enchede, The Netherlands, 13-15 September 2000