Security Control Schemes for Pervasive Medical Environments

Petros Belsis[1,2] Stefanos Gritzalis[1]
[1] Laboratory of Information and Communication Systems Engineering *(Info-Sec-Lab)*
Department of Information and Communication Systems Engineering
University of the Aegean, Samos, Greece,
{pbelsis, sgritz}@aegean.gr
[2] Department of Informatics
Technological Educational Institute (T.E.I.) of Athens, Greece

Abstract

The emergence of pervasive infrastructures and their continuously growing applicability to a variety of environments, poses new challenges relative to the secure management of users and data over volatile mobile ad-hoc networks. Among else, interconnected medical domains can utilize pervasive, wireless-based infrastructures. In this paper we argue about the necessity for reconciliation of traditional security models in order to adjust to pervasive infrastructures; we also consider a policy-based security framework that takes under consideration the increased privacy-related requirements of medical wirelessly interconnected domains.

1. Introduction

Pervasive environments from experimental technology tend to become commonplace, adopted as a non high-cost solution for a variety of environments, due to their relative easy deployment in terms of human effort and necessary budget and due to the continuous raise in computational power of handheld devices utilised for their realization. From their emergence, many types of applications and environments can benefit. Among them, the medical domain can suffice, by providing location independent timely accurate information, within predefined range, or alternatively across wirelessly interconnected domains. The volatility of these environments confronts developers with contradictory requirements:

- To provide access from anywhere to anyone authorised to use medical related information,
- Ensuring at the same time non-disclosure of treatment-related information to non-authorised persons.

Pervasive environments integrate a variety of heterogeneous applications, and demand flexible management of resources, available to wirelessly interconnected users and devices. Policy based management has supported efficiently the secure management of target resources which often span the borders of an organizational domain. Static oriented security management solutions become inapplicable in our case for a variety of reasons: large number of participant users, mobility of users and devices, necessity for flexible, context related applicability of access control decisions. Additively, policy based security models demand a redesign due to the unstable character of pervasive environments.

The proliferation of these innovative technologies and the presence of wireless interfaces expose network assets to a series of potential threats. Transient presence of nodes contributes to additive complexity as it makes difficult task their enumeration in advance.

Our research approach is two-fold:

- it attempts to establish a framework for the provision of e-healthcare services over pervasive environments
- it attempts to enhance the security robustness of such a wireless infrastructure and to overcome limitations of static access control methods.

The rest of the paper is organized as follows: Section 2 presents the design requirements, which direct our approach, relative to policy and topology specific demands. Section 3 discusses the basic notions behind the security models and their adjustment to the pervasive scenario. In Section 4 we discuss our extended RBAC model in order to support a pervasive multi-domain scenario. Section 5 describes the challenges that affect the applicability of these models for effective identification and manipulation of medical data. Section 6 presents related work in the area of wireless medical infrastructures. Section 7 describes a prototype implementation overview, while Section 8 concludes the paper.

2. Design requirements

Pervasive environments are built over mobile ad-hoc networks (MANETs), which are characterized by instability due to the mobility of participating nodes, while mobile devices do not excess in computational resources. They can be applicable in the case of medical domains, such as hospitals, enabling thus access to patient related information from all places within the hospital's wireless network range (Fig. 1). The sensitivity of the data related with patient's medical history imposes a number of additive requirements mainly privacy-oriented to be taken under consideration, while it is also urged through legislation in many countries.

2.1. Privacy preservation

A lot of portable devices nowadays enable user authentication using PKI (Public Key Infrastructure) keys. User authentication at device level is enabled by entering a PIN identifier, while the private key can be carried in a secure removable media, which enables the matching of the holder's identity with that of the owner. Even though computational resources are a burden for handheld devices, 128-bit symmetric encryption is supported by many manufacturers. It is possible to encrypt all necessary data, while the identification of both communicating parties can be verified through digital certificates.

2.2. Policy storage

There are variant approaches relative to policy storage and enforcement on handheld wireless devices. According to [1], policies can be stored on smart cards while the device can monitor all the time whether the smartcard is removed from the system or not. In our approach not all the devices need to be aware of the organizational policy, since not all the devices would enable provision of services for users or devices. The policy is maintained on special modules, the Policy Decision Points (PDPs) which reason about a user's access privileges over shared assets - mainly medical records -, which are kept only in distinct locations and where security controls are applied prior to any authorization. Instead of making the policy available to any device, we just make it available on critical points, which store medical information and where any misuse can lead to breaches of confidentiality and every access request is accompanied by provision of requester's credentials that are therefore evaluated according to the organizational policy.

2.3. Network topology

Our aim is to provide a solution that accomplishes the objective of providing anywhere anytime within a medical multi-domain environment access to critical information, providing secure delivery to authorized users only. Several challenges of socio-technical nature affect the design choices in such architecture.

Pervasive environments are being characterised by extensive number of users, making in general security management a complex task. Several approaches consider trust-based solutions [2] in order to manage security aspects. Our aim is not to provide to all the mobile users - within the medical domain - access to services, but to realize through the ubiquitous environment, access to those who are engaged in the treatment process and therefore to materialize the provision of better quality healthcare services, while minimizing the time-cost necessary to access medical related information.

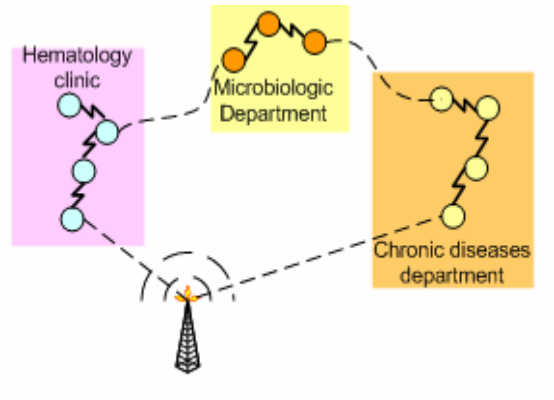

Fig. 1 Pervasive medical domain infrastructure

Policies provide a flexible solution for role and resources management, which can be spread across organizational boundaries. We mainly confront ourselves to the main principles of the Role Based Access Control (RBAC) model [3]. Though, the particularities of the framework discussed, pose new challenges and demand modifications to the standardized RBAC, as well as to most of the existing policy-based management frameworks, which have emerged so far. We consider a number of such modifications that among else demand determination of location and context based association of roles, time periodicity, as it will be discussed in the following paragraphs.

3. Policy based management framework

3.1. Extended RBAC model

The basic notions behind the RBAC model are users, and sessions (Fig. 2). To extend the support for least privilege, sessions are introduced. Sessions serve the case where a user signs on a system to perform some specific task. Sessions introduce some abstraction between users and roles. Therefore, sessions enable users to activate temporarily different roles, or to log with two or more roles at the same time.

Several modifications and extensions to basic RBAC are necessary to adjust it to multi-domain environments [17]. The nature of pervasive environments and the unstable character of wireless connections add additive restrictions and demand flexible modifications, incorporated in our framework, that:

- Are pre-settled by the system administrator, and that the user must specify in order to be granted authorization to activate a role (parameters domain specific mainly, that correlate a user with a specific domain
- Enable time periodicity, for example allow access within pre-specified time-intervals
- Enable context based role-assignment and role correlation for roles specified in different domains.

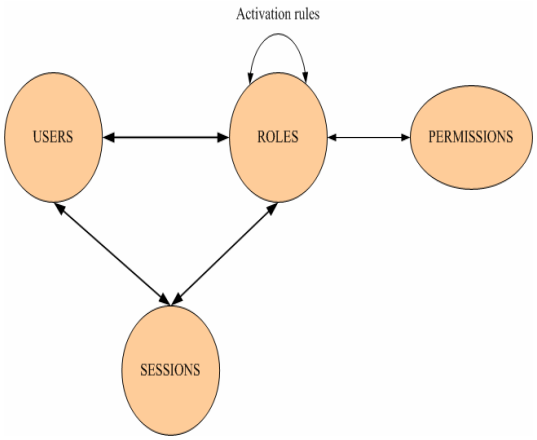

Fig. 2 Basic RBAC concepts

3.2. Role mapping across domains

A basic issue is related with the concurrent treatment of security parameters between autonomous self-managed (on terms of security policy) domains. For example, a doctor may be appointed to work as a manager on one clinic and also as a general practitioner on another. In order to be able to perform the necessary actions on each system, there has to be a way to enable her to provide her credentials and to be granted access on both systems, no matter of her location. A basic obstacle is related with the fact that different organizations have different organizational schemes - roles in general - and also different privileges assigned to each role. The subject of automating a negotiation procedure that would result in performing automatically a matching between the roles, their security attributes and their mappings can be proved to be NP-complete [4]. Many approaches have been proposed, others semi-automated [5], others focusing on providing a scalable and efficient solution, even with human interventions to some extent. We believe that the sensitivity related with protection of medical data, as well as the legislative restrictions make the automated negotiation procedure - due to the consequences in case of wrong mismatching between roles - an endangered solution and therefore other approaches, less error prone should be adopted at least in the case of medical interconnected domains. Therefore, we create a role hierarchy, to which the local role representation schemes need to conform, and the administrators who are aware of the legal and technical implications of the mapping are responsible to perform a correct mapping between the collaborating domains. In our case, the administrators will create from the beginning a role mapping between the different organizational policies, through the general intermediating mapping scheme. This mapping scheme acts as a federal, and all the domains that want to cooperate need to be mapped as subordinate to it (Fig.3).

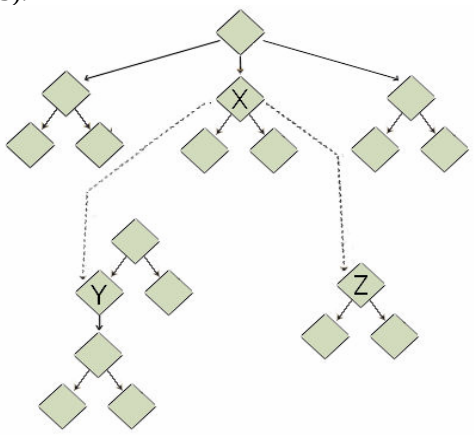

Fig. 3 Role-mapping across different domains. The role X on the federal role hierarchy scheme maps on role Y on domain's B hierarchy and role Z on domain's C role hierarchy scheme.

3.3. XACML framework

In our approach we utilize the Extensible Access Control Markup Language (XACML) [6]. XACML is a policy language that supports prohibitions, obligations, and resolution of conflicts. Its expressiveness and XML [12] (Extensible Markup Language) codification support allow its integration on a variety of environments, such as web-service based environments, distributed autonomous systems, and with some modifications to be applied also to pervasive environments. Among XACML's strong points, are:

- It is standardized and it is open, allowing extensions that enable interoperation between various platforms
- It is codified in (XML) which tends to dominate as codification standard and is operating system independent.
- It allows extensions as to support the needs for a variety of environments.
- It allows context based authorization, which is a big advantage

XACML implementations consist of several modules, with different roles each (Fig. 4). In a pervasive environment, the basic XACML module would demand adjustment to the topology-specific characteristics, as well as to the limited resource and processing power capability of the participating devices.

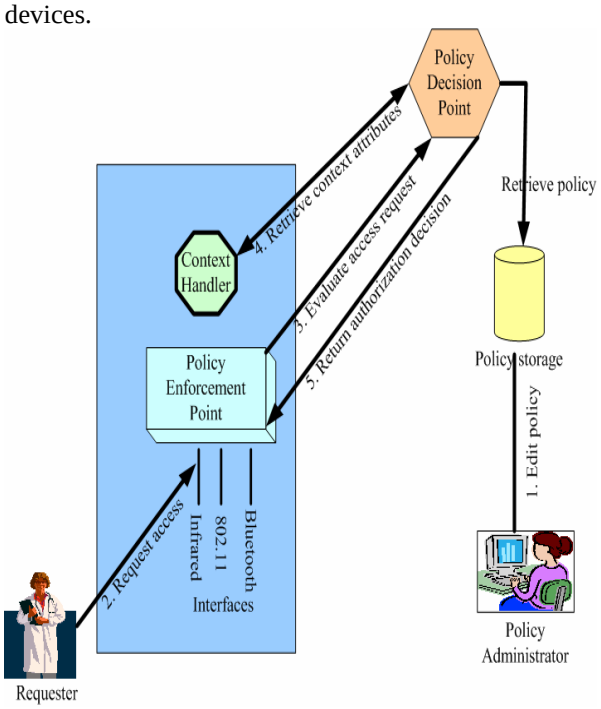

Fig. 4 XACML's pervasive infrastructure adjustment

Every request is directed to the domain's medical information database, which is restricted by the Policy Enforcement Point (PEP). The PEP forwards the request to the PDP, which collects context-related information through the context handler. We additively introduce time-periodicity related attributes to the parameters the context handler collects, while in the cases the requester is making the request from another domain -through the policy mapping- his role is adjusted to the permissions of the corresponding role on the domain where the medical information is stored. The PDP then acquires all context information, the corresponding role for the new domain and loads the local policy and evaluates the request against the policy. In our environment, node instability can cause temporal unavailability between the PEP and PDP. The default policy is prohibition in any case, while in order to prevent the unwilling unavailability scenario, as described in [7] we attempt to prevent link breakages based on a probabilistic calculation of the Link Expiration Time (LET), according to the input from transmission power samples measured from packets received from a node's neighbors [8][9]. Prior to a link breakage the node that identifies a link-expiration transmits a flood message, and accordingly there is an attempt for topology reconciliation between the active nodes.

4. Medical information management in pervasive environments

4.1. Asset identification in pervasive scenario

In order to identify and make available to all users assets from different organizations we have to enable semantic searching. Limited resources and bandwidth are also a problem, urging towards enabling ways for effective direction of query messages to the domain, which is more likely to contain information. Instead of flooding the network with query messages, which would limit the scalability potential of our system, we utilize domain ontologies, which contain subset of the information located in the domain (Fig. 5). For example in order to pose a query about a chronic disease and its symptoms, it would be more efficient to direct the query only to the specialized domain. This reduces both the response time as well as the overhead on the network bandwidth usage. Therefore, a user query will first be mapped on the ontology and then it will be flooded to a significantly smaller number of artifacts in the pervasive environment.

Another challenge is interconnected with the fact that by utilizing a security policy language codified in a semantic Web Ontology Language, we could grasp

more effectively from the benefits of semantic web [11]. Though XACML does not support directly speech acts, software agents can embed in their agent communication language access control oriented messages adjusted to the XACML syntax as well as they can utilize the ontologies in their agent-language communication messages [10].

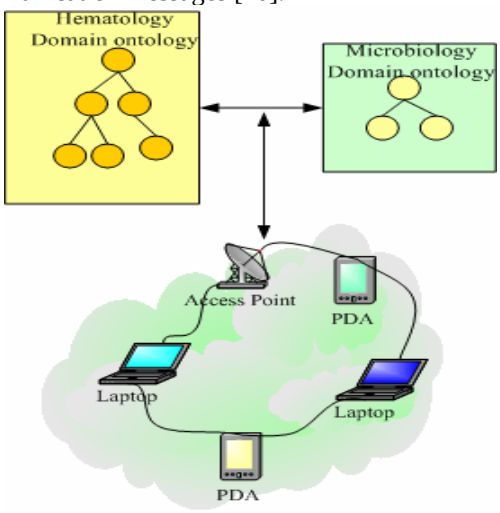

Fig. 5 Ontology-aided asset identification

4.2. Healthcare records codification and security related issues

Medical records can follow various formats and can be encoded in different data types. In order to achieve easy integration in many applications and codification in platform independent format, we adopt the XML language. Table 1 shows part of a medical record, containing information about a patient's treatment.

Medical records and other treatment-related information are stored in several locations within each domain. On every medical data storage point we create a PEP responsible for enforcing the domain's policy. The PEP is directing the message to the nearest PDP, which evaluates the request and the user's role-related attributes against the domain's policy and accordingly authorizes or not the request. In case of link breakage between the PEP and PDP then the authorization is not granted, due to the sensitivity of the patient's treatment information.

```
<medical>
<PatientID> 0304 </PatientID>
<treatment>
<drug>
<name>methylphenidate-
hydrochloride</name>
  <dailyDosage>30mgs</dailyDosage>
  <startDate>2005-3-4</startDate>
  </drug>
  <comment>patient exhibits side-effects
of skin coloration </comment>
  </treatment>
  <result>  <test>blood pressure</test>
  <value>120/80</value>
  <date>2005-03-02</date>
  <performedBy>Dr Smith</performedBy>
  </result>
  </medical>
```

Table 1 XML encoded patient record excerpt

5. System utility scenarios

We can consider the following scenario: A doctor within domain A is in the intensive care unit where she notices an unexpected change in a patient's monitored values. She notices instability susceptible to be connected with some hematological malfunction. In order to acquire information about the patient's history that is kept in the hematology department she uses her PDA and poses a query choosing among thematic categories which are available relative to the hospital domain ontologies. Her query is evaluated against the available ontologies from the hospital's different clinics. She also identifies the patient's SSN and sends the query that is directed through the pervasive graph to the hematology domain. The request is accompanied by the doctor's credentials and her role in the surgery domain. The hematology PEP advises the nearest PDP, and with the aid of the local context handler, the surgeon's role on the surgery department is correlated with an appropriate role on the hematology department. The new role clearance level is evaluated against the hematology department local policy and the patient's hematological record is retrieved. All communication is end-to-end encrypted by applying 128-bit encryption.

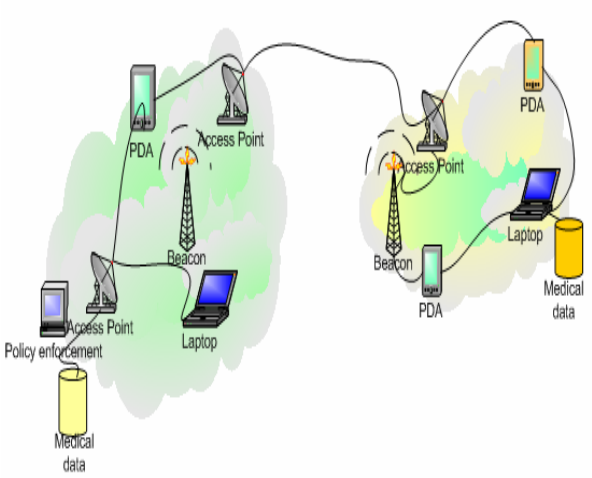

Fig. 6 Pervasive medical multi-domain interconnection / overall architecture. The presence of a beacon on each domain can notify the device about the local policy enforced and direct easier user-authentication.

6. Related work

Electronic health records management attracts significant international interest [13] and sets the scenery for the establishment of a distributed, coalition-based, security policy enhanced records exchange framework among different medical domains.

Wireless mediCenter [14] 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 [15] 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

In [2] a trust-based infrastructure is based for electronic healthcare redaction in pervasive environments. Our approach utilizes well-defined organizational policies and introduces role mappings across domains in order to facilitate the socio-technical implications of role and user mapping that can be quite difficult to manage in trust-based infrastructures and can be dangerous in critical environments such as medical environments.

7. Prototype Implementation overview

In order to test the validity of our approach, we created a preliminary scenario with four portable Intel Centrinos, and two Compaq PDAs. Each device was equipped with a user-indicant digital certificate, which accordingly was associated with a domain role. Apart from the user's role certificate the devices were equipped with a number of certificates that enables them to identify the domain in which they are at any moment by receiving digitally signed messages transmitted from a beacon (fig. 6). Therefore, the devices are aware constantly according to the received messages whether they are in the default domain, whether they are present in a collaborative domain or whether they are in a non-trusted zone. We experimented based on 802.11b environment, by creating a number of roles and edited policies for two domains. The policies were edited in XACML as described in previous section. The role of the medical-records database was played by two portables, which belonged to a different domain each one. The security modules were implemented in Java, as well as the software agent modules which act as mediators of the requester as described in [10]. We used the J2ME Java platform in order to minimize resource consumption. We created simple medical records in XML, and accordingly posed queries from each domain to acquire specific medical records based on the patient's id. By choosing from the main menu among predefined terms, a query is directed to the appropriate domain and local ontologies are retrieved. The ontologies are edited in Resource Description Framework (RDF) language [18]. In our scenario requests were directed from both networks within the same domain or form one domain to the other. A beacon transmitting in predefined time-intervals messages enables the device to identify the presence within the default network's limits or to trigger the role mapping procedure. Network identification is enabled through the predetermined keys, which are stored in the mobile devices. When it is not possible to receive a message within the pre-settled time limits, it is presumed that the device is out of range and the link is considered broken. Each request is accompanied by the most recently received beacon transmission message, and the user's role credentials. The response will be efficiently encrypted, as well as all the information exchanged between the PEP and the requester. For each domain we created three roles, with different security clearance and

attributes over the medical records, such as Read, Modify, Create, the nurse role having the minimal the WardManager the maximal rights. We sent queries for patient's records within one domain and towards the other domain. Therefore, through our policy mapping implementation scheme we achieve a scalable and robust solution towards access control enforcement, while by means of PKI based encryption we achieve confidentiality and non-authorized data disclosure. Our approach enables transparent and secure access to authorized users, without necessity to develop specific portals as in [14] and is policy based management framework is not restricted by the limitations of access control lists as in [15]. We additively enable location based device and user identification, while we extended the basic RBAC model so as to include the extended functionalities and to adjust to the peculiarities of multi-domain pervasive interconnected environments.

8. Conclusions

In this paper we discuss the application of pervasive environments for medical interconnected domains, as well as the limitations of traditional access control schemes towards their applicability on this area. We present our concept implementation and provide a security framework for enabling multi domain medical record identification and secure dissemination. We utilize interoperable platforms for both storage of medical records and policy management and we present the necessary extensions.

We intend to apply our scenario to a wider extent and to measure our platform's performance through extensive testing and recording of efficiency parameters. In order to test the scalability features support for our environment, we plan in the near future to expand the measurements through simulation, based on the MobiEmu [16] emulation environment. We also intend to extend the wireless infrastructure by incorporating devices with limited resources.

Acknowledgments

This work was co-funded by 75% from EU and 25% from the Greek Government under the framework of the Education and Initial Vocational Training Program *Archimedes.*

9. References

[1] W. A. Jansen, T. Karygiannis, S. Gavrila, and V. Korolev. Assigning and Enforcing Security Policies on Handheld Devices. In Proceedings of the Canadian Information Technology Security Symposium, May 2002

[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] R. Sandhu, D. Ferraiolo, and R. 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

[4] V. Bharadwaj, J. Baras Towards Automated negotiation of Access Control Policies, 4th International Workshop on Policies for Distributed Systems and networks (Policy 03), 2003, IEEE Press

[5] A. Herzberg, Y. Mass, J. Michaeli, D. Naor, and Y. Ravid. Access control meets public key infrastructure, or: Assigning roles to strangers. In Proceedings of the IEEE Symposium on Security and Privacy, Oakland, California, May 2000, IEEE Press

[6] 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

[7] A. Malatras, G. Pavlou, P. Belsis, S. Gritzalis, C. Skourlas, I., Chalaris Secure and Distributed Knowledge Management in Pervasive Environments, in Proceedings of IEEE International Conference on Pervasive Services, July 2005, Santorini - Greece, IEEE Press.

[8] P. Agrawal, D.K. Anvekar, and B. Narendran, Optimal Prioritization of Handovers in Mobile Cellular Networks, *Proceedings of the Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communication (PIMRC)*, The Hague, Netherlands, September 1994, pp. 1393-1398

[9] B. Narendran, P. Agrawal, and D.K. Anvekar, Minimizing Cellular Handover Failures Without Channel Utilization Loss, *Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM)*, San Francisco, CA, December 1994, pp. 1679-1685

[10] P. Belsis, A. Malatras, S. Gritzalis, C. Skourlas, I. Chalaris Pervasive Secure Electronic Healthcare Records Management, in Proceedings of the ICEIS 7th International Conference on Enterprise Information Systems - Workshop on Ubiquitous Computing, S. K. Mostefaoui (Ed.), May 2005, Miami, USA, published by ICEIS

[11] A. Patwardhan, V. Korolev, L. Kagal, A. Joshi, Enforcing Policies in Pervasive Environments, Proceedings of the MobiQuitous 2004 First Annual Conference on Mobile and Ubiquitous Systems: Networking and Services, IEEE Press.

[12] Extensible Markup Language Specification (XML), http://www.w3.org/XML/

[13] R. E. Scott, P. Jennet, M. Yeo, Access and authorization in a Global e-Health Policy context. International Journal of Medical Informatics (2004) 73, 259-266

[14] Wireless Medicenter. http://www.wirelessmedicenter.com/mc/glance.cfm
[15] D. Brazier, Alpha Bravo Charlie Ltd. The m-care project. http://www.m-care.co.uk/tech.html
[16] Y. Zhang, Li, W., An Integrated Environment for Testing Mobile Ad-Hoc Networks, ACM MobiHoc 2002, ACM Press
[17] J.B.D. Joshi, R. Bhatti, E. Bertino, A.Ghafoor Access Control Language for Multi-Domain Environments, IEEE Internet Computing, November/December 2004 (Vol. 8, No. 6)
[18] D. Brickley, R. V. Guha, Rdf Vocabulary Description Language 1.0: Rdf schema, Tech. report, W3C, January 2003.