Towards Differentiated Utilization of Attribute Mutability for Access Control in Ubiquitous Computing

Christos Grompanopoulos, Ioannis Mavridis
Department of Applied Informatics
University of Macedonia
Thessaloniki, Greece
groban@uom.gr, mavridis@uom.gr

***Abstract*- The operational characteristics of ubiquitous computing environments (UbiCom) generate new access control requirements which existing classical access control models fail to support efficiently. However, the Usage Control (UCON) family of models introduces components and mechanisms that seem to be able to partially match the specific requirements imposed by UbiCom environments. In this paper, an evaluation of current access control models based on a brief study of UbiCom access control requirements is presented. Then, a new access control approach that extends UCON towards a differentiated utilization of attribute mutability for easiness of administration, better performance and lower operational cost in UbiCom environments is proposed.**

***Keywords*- access control; ubiquitous computing; UCON; context; attribute mutability.**

I. Introduction

Over the last years a lot of devices with small dimensions and remarkable computing capabilities have been presented. Such devices are able to communicate with each other even in the absence of an infrastructure network, through the creation of mobile ad-hoc networks (MANETs). Additionally, most of these devices use sensors to capture values of parameters that characterize the execution environment, in order to provide personalized functionality without user's conscious mediation [1]. Such computing environments are coming closer to Mark Weiser's [2] vision concerning ubiquitous computing (UbiCom).

Traditional access control approaches, e.g. Mandatory Access Control (MAC), Discretionary Access Control (DAC) and Role-Based Access Control (RBAC) [3-4], base their decision making on user's static credentials like identity, rank or role set. However, using an access control decision mechanism based only on static user credentials is not appropriate in UbiCom since users are either anonymous or there is no knowledge about their previous behavior. Moreover, since transactions in UbiCom can take place in a variety of environments, access control does not only depend on the identity of the requestor but may also vary due to environmental factors, for example user's location or transaction's time period.

Instead, a more appropriate approach is the use of properties (attributes) that characterize not only users and resources but also the environment in which the action takes place. The UCON model presented by [5] uses subject and object attributes in the access control decision making process and provides the capability not only to control attribute information before but also during the execution of the permitted access. Furthermore, attributes in UCON can be either immutable or mutable as a result of such a permitted access to information or other resources.

The large number of subject and object attributes, as a result of portability and mobility, along with the vast amount of environment and systems (contextual) information, usually collected through networked sensors, have increased significantly the complexity of access control decision mechanisms in UbiCom. Furthermore, the mutability of attributes combined with frequently changing systems and environmental values imposes a high operational cost to UbiCom access control systems. This paper aims to propose an approach that utilizes attribute and context mutability in order to eliminate operational cost for access control decision making in UbiCom environments. Section II presents a brief study of access control requirements in UbiCom through a motivating scenario and related literature. Section III discusses the advantages and disadvantages of the dominant families of access control models of latest years: RBAC and UCON. Section IV proposes a classification of attributes based on their mutability and the corresponding use of this classification in a new access control framework that extends UCON. Section V concludes and outlines future directions.

II. Access control requirements

To obtain the access control requirements arising from ubiquitous computing environments, the following scenario is used. In a research institute, employees and potential visitors use PDA's for everyday operations. The user's position is captured though sensors. Users can use the appliances of the institution, if applicable based on a set of rules. These rules might consist of context information as the user's physical presence in the room, where the machine is located or time constraints such as working hours. It is also possible for the employees of the institution to request usage resource of another institution.

The characteristics of UbiCom environments, as described in [6-8] and presented through the previous scenario, introduce a series of requirements for access control models, mechanisms and policies, as follows:

- **Support of partially unknown-users**

  As described in the scenario, users may not be employees of the institution, so their identity might be unknown. As a result, it is necessary that the establishment of an access control decision may not be based using only the user's identity but also the user's attributes [8]. This gives greater flexibility in the access control system to support partially unknown users. Both attributes assigned in the form of credentials and also history information of transactions with other authenticated users can lead to the creation of trust [9-10]. Trust among users can be used for setting access control decision criteria.

- **Cooperation among heterogeneous entities**

  A typical requirement, which derives from the scenario and also has been reported in earlier work [11], is the desirable cooperation among different administrative authorities. In the extreme situation, every user is an authority by its own. In order to achieve collaboration, a common language for the description of access control policies and entity attributes, is necessary [8].

- **Using context information**

  Another requirement, which derives from the scenario and also has been reported in earlier work [12-15], is related to the use of contextual information during the access control decision making process. The existence of a mechanism responsible for the accurate in-time collection [16] and evaluation [17] of contextual information before its use, is essential. Additionally, access control policies should have the ability to incorporate context modeling and conditions in their rules [18].

- **Adaptation of operation changes**

  A core feature of UbiCom environment is the frequently modification of their operational characteristics. This is due to the dynamic nature of contextual information (time, entities co-located, available bandwidth, etc.), constant user's movement and applications, data and devices availability [7]. This fact imposes the existence of the capability of decision mutability even during the usage of resources, as described by the usage control model. For example, an employee in our scenario should not have access to the assets of the company during non working hours, or when he moves from one room to another. Additionally, policies should be altered as a result of environmental changes [19-20].

- **Protection of privacy**

  One of the requirements, which to a large extent will determine the success of UbiCom environments, is the protection of privacy [6]. Portable devices are used by users in all aspects of their daily life and not just for professional reasons. Consequently, disclosure of user's personal information will have a major impact on them. Users must feel that they control their personal data without requiring this procedure a great effort from them. Research work concerning the protection of privacy in UbiCom was published in [21]. Moreover, contextual information collected by networked sensors must also be protected as part of user's personal information [22].

- **Ease of administration**

  The new computing paradigms realized in UbiCom environments impose new requirements, since they support a wide range of daily functions performed by users who may not have enough knowledge of the technologies they use for. One of these requirements is the need for automatic generation of access control decisions [23] to such an extent that their operation is not perceived by the user. Additionally, access control policies must be declarative to descriptive the complexity of these environments but also simple enough to be supported by users with no prior technical knowledge [24].

- **Resource constrained operation**

  Furthermore, technologies used in UbiCom impose limitations in the selected security solutions [7]. UbiCom devices run on batteries and have limited computing resources. Even the communication (usually wireless) technologies and protocols provide limited bandwidth and are characterized by frequent disconnections. The constrained resources offered by UbiCom devices deter the use of highly secure and complicated solutions (e.g. public-key infrastructure - PKI). Thus, they demand the use of lightweight solutions for access control models, mechanisms and algorithms, in order to consume less power, CPU and memory. Additionally, low bandwidth creates the requirement to minimize the communication overhead among participating parties.

III. Evaluation of Current Access Control Models

A. RBAC

One of RBAC's main elements is the notion of role [3]. Each user is assigned to roles via a User to Role Assignment (URA) relationship. Accordingly, the Permission to Role Assignment (PRA) relationship entrusts permissions to roles. Permissions in RBAC are a combination of an operation on a specific object. Roles can be organized into hierarchies giving the opportunity for senior roles to inherit permissions from junior roles.

One of RBAC's virtues [23] is the support of the abstraction concept, which allows its use by a wide range of applications. Furthermore, RBAC supports the principle of least privilege, separation of users and permissions to role assignments, and finally separation of duty, which enforces restrictions on the roles that a user can be assigned to or activate. Additionally, RBAC provides low operational cost because its access control decision making is based only in the possession of a role by a user. Moreover, the ease of administration in RBAC model is a significant reason for its great acceptance by professionals.

However, RBAC presents a number of disadvantages, which researchers have attempted to eliminate with appropriate extensions. One of these drawbacks is that RBAC fails to support contextual information during the access control decision making process [11-12]. In addition, the assignment of users to roles, and roles to permissions is performed only through the involvement of the system administrator, making so nearly impossible the application of RBAC in distributed environments with a vast amount of users, e.g. the Web [25]. Finally, new requirements for next generation RBAC models [23] include the ability to control resources not only before but also during access. Furthermore, future RBAC should support the concept of accountability in case of deviation of a user from the correct use of resources.

B. *UCON*

The UCON family of models [5] introduces eight core components viz. subject, object, subject attributes, object attributes, right, authorizations, obligations and conditions. Subjects and objects are used in the same sense as in RBAC but they are described by attributes. Access control rules are classified into three categories: authorizations based on the attributes of subject and object, obligations in the form of actions that the user is required to accomplish before access, and conditions to describe environmental and system related restrictions that must be met.

A key advantage of UCON is the ability to enforce access not only before but also during access. Also, support of attributes during the access control decision allows a more detailed control for the administrator. Finally, attribute mutability feature makes possible the alternation of the set of permissions that a subject can hold as a result of his actions.

Among the disadvantages of UCON is the lack of administrative background work. Additionally, since the process of access control decision making is based on attributes, it produces a vast computational cost each time an access is attempted. Furthermore, the use of attributes generates complex access control policy rules. Finally, little research [26] has been done on developing consensus on a UCON application framework.

TABLE 1 EVALUATION OF RBAC & UCON

Model	Advantages	Drawbacks
RBAC	• Ease of administration • Large implementation base • Separation of URA & PRA • Separation of duty • Least privilege	• PRA, URA with administrator support • Course grained access control • Lack of context support • Control only before access
UCON	• Control before and during access • Fine grained access control • Attribute mutability	• Lack of Administrative models • High Operational cost • Complex policies • Small implementation base

The major advantages of the UCON family of models, as depicted in Table 1, is the ability to support usage control and attribute's mutability, making UCON a proper candidate for use in UbiCom environments. However, the high operational cost imposed by UCON possibly makes its implementation quite difficult in UbiCom constrained resource environments, especially considering MANETs. Our research work aims to propose a solution that is based on the core characteristics of the UCON model but extends it with functionalities that meet the requirements for access control in UbiCom environments, as presented in the previous section, in order to achieve low operational cost, simpler policies and ease of administration.

IV. THE PROPOSED APPROACH

A. *All is attributes*

Firstly, we introduce attributes for storing and manipulating contextual information. For example, suppose that a policy rule suggest that a user can have access to a remote server, only during working hours. If the server is located to a country with different time zone, time can be derived by the location either of the user or the remote server. In the UCON family of models, contextual information is used in conditions, and separated from user and object attributes. However, context is described as any information relevant to the interaction between two entities, including entities themselves [27]. This can lead to the conclusion that context is not irrelevant to the entities such as subjects and objects, but it can be assigned directly to them.

Stating that contextual information can refer directly or indirectly to the subject or the object of access leads to the selection of context representation using only attributes. Consequently, the existence of conditions as specified in the UCON model is no longer necessary. UCON authorizations now must include rules that use not only attributes of subjects or objects but also information of the environment and system conditions referred to them.

Last but not least, the resolution of attribute values, which describe contextual information, is performed using an independent context middleware component.

B. *Mutability degree*

The values of the attributes that characterize objects and subjects should not be considered unchanged. Rather, their nature is variable due to contextual information. Contextual information, described by the aforementioned attributes, is expected to change frequently [28].

Attribute mutability as defined in UCON is another factor that affects the values of attributes. According to the above observation, a classification can be made based on the frequency of changes of attribute values. Some attribute values are frequently changing (i.e. time). Nonetheless, others are changing rarely (i.e. a user's age) and their value could also be considered constant for a given time span. Thus, each one attribute is characterized as frequently changed attribute (FCA) and rarely changed attribute (RCA).

Based on the FCA and RCA classification, the following extension to the respectively model is proposed, as depicted in Fig. 1. Subjects (S), Objects (O), Rights (R), Authorizations

(A) and oBligations (B) are used with the same sense as in UCON family of models. The values of attributes for subjects and objects are collected either from the particular system or the current environment. Subsequently, FCAs are used in the definition of conditions. The second type of attributes (RCA) is used for the automatic assignment of subjects and objects to states, as frequently specified in the access control policy. Access decision making is based on a combination of subject states, object states and conditions.

The advantage of the proposed approach is that during the access control decision process, only the evaluation of conditions is required. Additionally, conditions evaluation is not necessary if the required states are not assigned to subjects or objects. State assignment is based on rules and is not required to be performed for every access but in longer time intervals. Consequently, the proposed approach requires low operational cost for access decision. This is a key requirement in UbiCom environments.

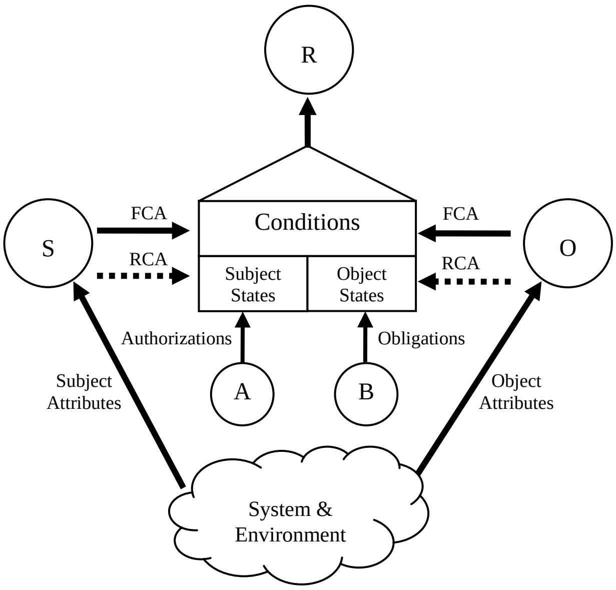

Figure 1 Differentiated use of attributes based on their mutability

C. Access control framework

The proposed framework for access control in UbiCom is defined based on the concepts of Access Decision Function and Access Enforcement Function (ADF and AEF respectively) [29]. ADF is the entity responsible for creating the access control decision, while AEF for its enforcement. ADF is composed by the Evaluator and Dynamic State Assignment components. The Evaluator is responsible for the communication with other entities and for the evaluation of conditions. Dynamic State Assignment as its name suggests relates subjects and objects with states based on rules, which use their RCA. The proposed access control framework is illustrated in Fig. 2, as follows:

- The RCAs of every subject or object identified in the UbiCom environment are sent to the Access Decision Function, and more specifically to the Dynamic State Assignment component. These attributes are processed according to predefined rules in order to assign states to corresponding entities.
- Subsequently, each time a subject asks to access an object, it sends a request to ADF, including his FCAs, the name of the object he wants to access and the type of access operation.
- The Evaluator after receiving the access request extracts the policy rules that authorize use of that object.
- The Evaluator collects subject and object states from the Dynamic State Assignment component, and checks if the policy rules are satisfied. If not, a deny response is propagated to the subject and AEF. Otherwise the following steps are executed.
- Based on the Conditions used in the policy rules, the included FCAs are denoted. The Evaluator collects attribute values either by asking objects or from the context middleware. Then, it calculates the predefined conditions.
- Following, the Evaluator component calculates the access control decision based on the subject and object states and the conditions evaluated in the previous step.
- The final access decision is sent to AEF.

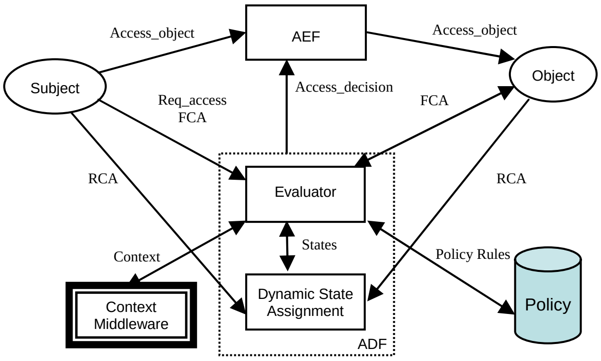

Figure 2 Access control framework

V. CONCLUSION

The first objective of this study was to highlight the requirements for access control systems in UbiCom environments. Based on the above requirements, the UCON family of models was selected for use in UbiCom environments, due to its capability to support continuity of decision and attribute mutability. However, the dynamic nature of contextual information and the vast amount of mutable attributes result in high operational cost and complexity of the supporting policy languages, thus making UCON difficult to be implemented in UbiCom environments. To overcome these problems, a new access control framework was presented, as an extension to the UCON family of models. The access control framework is based on a differentiated utilization of attribute mutability, as a result of an alternative representation of contextual information through subject and object attributes. In addition, subject and object attributes are classified into two categories to minimize the operational cost and speed up the calculation of rights and finally the access control decision making process in UbiCom environments.

References

[1] B. Schilit, N. Adams, and R. Want, "Context-aware computing applications," in Mobile Computing Systems and Applications, 1994. Proceedings., Workshop on, 1994, pp. 85-90.

[2] M. Weiser, "The computer for the 21st century," SIGMOBILE Mob. Comput. Commun. Rev., vol. 3, pp. 3-11, 1999.

[3] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, "Role-Based Access Control Models," Computer, vol. 29, pp. 38-47, 1996.

[4] S. D. C. d. Vimercati, S. Foresti, and P. Samarati, "Authorization and access control," in Security, Privacy, and Trust in Modern Data Management, ed: Springer Berlin Heidelberg, 2007, pp. 39-53.

[5] J. Park and R. Sandhu, "The $\mathrm{UCON}_{\mathrm{ABC}}$ usage control model," ACM Trans. Inf. Syst. Secur., vol. 7, pp. 128-174, 2004.

[6] K. Ranganathan, "Trustworthy Pervasive Computing: The Hard Security Problems," presented at the Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops, 2004.

[7] R. K. Thomas and R. Sandhu, "Models, Protocols, and Architectures for Secure Pervasive Computing: Challenges and Research Directions," presented at the Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops, 2004.

[8] E. Damiani, S. D. C. di Vimercati, and P. Samarati, "New paradigms for access control in open environments," International Symposium on Signal Processing and Information Technology, vol. 0, pp. 540-545, 2005.

[9] D. Artz and Y. Gil, "A survey of trust in computer science and the Semantic Web," Web Semantics: Science, Services and Agents on the World Wide Web, vol. 5, pp. 58-71, 2007.

[10] L. Kagal, T. Finin, and A. Joshi, "Trust-Based Security in Pervasive Computing Environments," Computer, vol. 34, pp. 154-157, 2001.

[11] J. Bacon, K. Moody, and W. Yao, "A model of OASIS role-based access control and its support for active security," ACM Trans. Inf. Syst. Secur., vol. 5, pp. 492-540, 2002.

[12] M. J. Covington, W. Long, S. Srinivasan, A. K. Dev, M. Ahamad, and G. D. Abowd, "Securing context-aware applications using environment roles," presented at the Proceedings of the sixth ACM symposium on Access control models and technologies, Chantilly, Virginia, United States, 2001.

[13] P. McDaniel, "On context in authorization policy," presented at the Proceedings of the eighth ACM symposium on Access control models and technologies, Como, Italy, 2003.

[14] D. Kulkarni and A. Tripathi, "Context-aware role-based access control in pervasive computing systems," presented at the Proceedings of the 13th ACM symposium on Access control models and technologies, Estes Park, CO, USA, 2008.

[15] C. K. Georgiadis, I. Mavridis, G. Pangalos, and R. K. Thomas, "Flexible team-based access control using contexts," presented at the Proceedings of the sixth ACM symposium on Access control models and technologies, Chantilly, Virginia, United States, 2001.

[16] M. Baldauf, S. Dustdar, and F. Rosenberg, "A survey on context-aware systems," International Journal of Ad Hoc and Ubiquitous Computing, vol. 2, pp. 263--277, June 2007.

[17] A. Ranganathan, J. Al-Muhtadi, and R. H. Campbell, "Reasoning about Uncertain Contexts in Pervasive Computing Environments," IEEE Pervasive Computing, vol. 3, pp. 62-70, 2004.

[18] F. Cuppens and N. Cuppens-Boulahia, "Modeling contextual security policies," Int. J. Inf. Secur., vol. 7, pp. 285-305, 2008.

[19] L. Kagal, T. Finin, and A. Joshi, "A Policy Language for a Pervasive Computing Environment," presented at the Proceedings of the 4th IEEE International Workshop on Policies for Distributed Systems and Networks, 2003.

[20] A. Toninelli, R. Montanari, L. Kagal, and O. Lassila, "Proteus: A Semantic Context-Aware Adaptive Policy Model," presented at the Proceedings of the Eighth IEEE International Workshop on Policies for Distributed Systems and Networks, 2007.

[21] H. S. Cheng, D. Zhang, and J. G. Tan, "Protection of Privacy in Pervasive Computing Environments," presented at the Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'05) - Volume II - Volume 02, 2005.

[22] K. Minami and D. Kotz, "Secure context-sensitive authorization," Pervasive and Mobile Computing, vol. 1, pp. 123-156, 2005.

[23] R. Sandhu and V. Bhamidipati, "The ASCAA Principles for Next-Generation Role-Based Access Control," in Proc. 3rd International Conference on Availability, Reliability and Security (ARES), Barcelona, Spain, 2008, pp. xxvii-xxxii.

[24] A. Joshi, T. Finin, L. Kagal, J. Parker, and A. Patwardhan, "Security Policies and Trust in Ubiquitous Computing," Philosophical Transactions of the Royal Society A, vol. 366, pp. 3769-3780, October 2008.

[25] M. A. Al-Kahtani and R. Sandhu, "A Model for Attribute-Based User-Role Assignment," presented at the Proceedings of the 18th Annual Computer Security Applications Conference, 2002.

[26] J. Park and R. Sandhu, "Towards an Engineering Framework for Usage Control and Digital Rights Management," ed: George Mason University, 2001.

[27] G. D. Abowd, A. K. Dey, P. J. Brown, N. Davies, M. Smith, and P. Steggles, "Towards a Better Understanding of Context and Context-Awareness," presented at the Proceedings of the 1st international symposium on Handheld and Ubiquitous Computing, Karlsruhe, Germany, 1999.

[28] G. Neumann and M. Strembeck, "An approach to engineer and enforce context constraints in an RBAC environment," presented at the Proceedings of the eighth ACM symposium on Access control models and technologies, Como, Italy, 2003.

[29] ITU-T, "X.812 Recommendation," in Data Networks and Open System Communications Security - Information Technology – Open Systems Interconnection – Security Frameworks for Open Systems: Access Control Framework, ed: ITU, 1995, p. 44.