Towards a Context-aware Framework for Pervasive Computing Authorization Management

Extended Abstract

Patroklos G. Argyroudis
Department of Computer Science
University of Dublin, Trinity College
College Green, Dublin 2, Ireland
Email: argp@cs.tcd.ie

Donal O'Mahony
Department of Computer Science
University of Dublin, Trinity College
College Green, Dublin 2, Ireland
Email: omahony@cs.tcd.ie

Abstract— **Pervasive computing environments have by definition three main inherent properties; extremely open and dynamic nature, suggesting large number of interactions among previously unknown entities, the ability to adapt according to perceived context information, and interaction interfaces that integrate naturally with the goals users are trying to achieve. Traditional security management approaches fail to capture the requirements of pervasive computing. Our proposed architecture, called *ÆTHER*, addresses access control and the establishment of security associations in pervasive environments by extending traditional trust management. We model permissions as the rights of authority sets that grow dynamically without requiring manual reconfiguration, and we define context-adaptive access control policies that are embedded into pervasive artifacts using the well-defined concept of location-limited channels.**

I. Introduction

Computing devices are being embedded into everyday appliances and become part of our environment. Interactions with such devices must be integrated with the purpose a user aims to achieve in a natural, graceful way in order to *feel* ubiquitous. However, the open nature of such environments raises security and privacy concerns that need to be addressed in a coherent manner along with the development of the required underlying infrastructure. Although the traditional security requirements remain the same, this new approach to computing has introduced additional challenges.

The main problem in addressing the security requirements of pervasive computing environments is the large number of ad hoc interactions among previously unknown entities, hindering the reliance on predefined associations. Another equally important problem is that the employed security solution should follow the ubiquitous computing vision and be naturally integrated with the actions the users perform in order to complete their objectives. A user that carries a multitude of devices must be able to establish spontaneous secure communication channels with the devices embedded into the environment or carried by other users without extensive manual reconfiguration tasks. Perceived contextual information from the environment should be employed in order to enable such communication needs.

Our proposed authorization architecture, named ÆTHER[1], has been designed specifically to address such dynamic context-aware environments where *a priori* knowledge of the complete set of participating entities and global centralized trust registers cannot be assumed. The basis of our work is the *role-based access control* (RBAC) model [5], according to which entities are assigned to roles and roles are associated with permissions. We have extended RBAC in order to allow the sets of entities that have authority over a specific role, or *authority attribute sets* (AASs) according to the terminology of ÆTHER, to grow dynamically. Furthermore, we associate permissions with *context attribute sets* (CASs) whose membership is determined dynamically and by using them we define context-sensitive access control policies.

II. The ÆTHER Approach

Our security management architecture provides a way for the owners of pervasive devices to specify autonomous authority domains and the security relationships that form the foundation of trust in them. Based on initial trust bootstrapped with location-limited channels we enable the establishment of dynamic secure associations with previously unknown pervasive entities. The extended Resurrecting Duckling security model proposed the imprinting of devices with policies that define the type of relationships the slave device is allowed by its master to have with others in order to address peer-to-peer interactions [6]. However, the authors simply proposed the use of trust management systems as a way to define imprinted policies without offering any specific engineering details. Furthermore, even the extended Resurrecting Duckling system defines a static association model between the master and the imprinted devices, limiting its direct application in situations where associations are established in an ad hoc manner. In ÆTHER we have extended these concepts and designed a complete authorization management system for dynamic context-aware pervasive computing environments.

An *authority domain* (AD) in the terminology of ÆTHER is defined as the initial set of relationships between attributes and principals specified in a security policy and is a logical representation of a pervasive computing environment. The owner of several devices creates an authority domain by specifying in a policy which principals are trusted to certify which

[1] The name was inspired by the medium that was once believed to pervade all space supporting the propagation of electromagnetic waves.

authorization and context attributes. The policy is embedded into the owner's devices via a location-limited channel such as an infrared link. Moreover, the owner creates policy entries for controlling what authorization and context attributes a principal must possess in order to get specific access rights to a resource provided by a device.

A. Authority Attribute Sets

The specific policy constructs that define the authority attributes of a domain and the principals that act as sources of authority for these are called *authority attribute sets* (AASs). In ÆTHER permissions are modeled as the rights of an AAS. We associate rights with actions, so possession of an authority attribute permits the certified principal to perform a certain action. The certification of the authority attributes is performed by the members of the corresponding AAS.

The AASs can be either static or dynamic. A static set can only have as sources of authority the principals specified in the initial policy entry. The set of principals that act as sources of authority for dynamic AASs can grow without requiring the explicit change of a policy entry or the issuing of a new one [1]. Hence, we provide decentralized administration of ADs and facilitate the effortless introduction of previously unknown principals. Furthermore, we provide a mechanism to allow the linking of ADs by mapping corresponding attribute sets for supporting secure interactions between different environments.

B. Context Attribute Sets

The concept of *context attribute sets* (CASs) provides a high-level interpretation of the low-level context information collected by sensors embedded into the environment. Membership of principals in CASs is maintained dynamically based on the raw data of context-aware sensor infrastructures, like for example the ones presented in [4]. Thus, whenever an access control decision is required that has been defined using a context attribute, the corresponding CAS is queried regarding the membership status of the requesting principal.

The access control policies that are embedded into pervasive devices define context attribute requirements or restrictions in addition to the ones using authorization attributes (see Fig. 1). This allows the specification of context-adaptive policies that control access to protected resources.

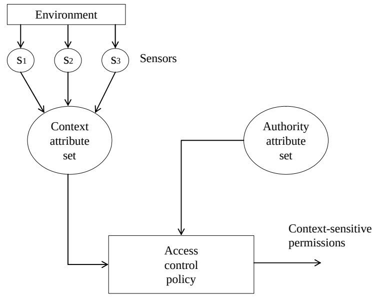

Fig. 1. Context-sensitive permissions.

However, the information regarding the membership of principals in specific CASs may be considered sensitive or private. In these cases we view the knowledge of membership as a normal resource to be protected and accessed only by properly authorized principals. The authorization can be handled by AASs or even CASs whose membership list is not considered sensitive in certain contexts. For example, a policy can specify that the membership list of the CAS that has authority over current location can be accessed by any principal that is in the same physical location as the location sensor. On the other hand, any principal in the owner AAS of the environment can access the same information disregarding its location.

III. Conclusion

One of the main advantages of using authorization attributes instead of capability-based credentials is that certificate distribution and initiation of delegation chains is not required when a new device is introduced into an authority domain, or when an existing device starts to provide a new service. The owner simply embeds the required policy statements into the new device and the principals that already have the required attribute credentials can start using it immediately via any communication medium.

During our initial investigation of the problem domain we completed a performance analysis of three security protocols, namely TLS, S/MIME and IPsec, on handheld devices [2]. The results show that the time taken to perform cryptographic functions is small enough not to significantly impact real-time transactions. Therefore the overhead of the cryptographic processes used in ÆTHER is no obstacle to its implementation on handheld devices. For our prototype we have modified the KeyNote [3] trust management system to add support for attribute certificates and the other ÆTHER policy constructs. We have also extended its inference engine to include support for dynamic attribute authorization decisions and integer delegation control for AASs.

References

[1] P. Argyroudis and D. O'Mahony, "Securing communications in the smart home," in *Proceedings of 2004 International Conference on Embedded and Ubiquitous Computing (EUC'04)*, ser. Lecture Notes in Computer Science, vol. 3207. Springer-Verlag, August 2004, pp. 891–902.

[2] P. Argyroudis, R. Verma, H. Tewari, and D. O'Mahony, "Performance analysys of cryptographic protocols on handheld devices," in *Proceedings of 3rd IEEE International Symposium on Network Computing and Applications (IEEE NCA'04)*, August 2004, pp. 169–174.

[3] M. Blaze, J. Feigenbaum, and A. Keromytis, "The keynote trust management system version 2," RFC 2704, September 1999.

[4] S. Ponnekanti, B. Lee, A. Fox, P. Hanrahan, and T. Winograd, "Icrafter: a service framework for ubiquitous computing environments," in *Proceedings of 3rd Ubiquitous Computing International Conference*, ser. Lecture Notes in Computer Science, vol. 2201. Springer-Verlag, 2001, pp. 56–75.

[5] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, "Role-based access control models," *IEEE Computer*, vol. 29, no. 2, pp. 38–47, 1996.

[6] F. Stajano, "The resurrecting duckling – what next?" in *Proceedings of 8th International Workshop on Security Protocols*, ser. Lecture Notes in Computer Science, vol. 2133. Springer-Verlag, 2001, pp. 204–214.