Workshop on Research Directions in Situational-Aware Self-Managed Proactive Computing in Wireless Adhoc Networks

Context-Aware Access Control for Mobile Users (Position Paper)

Isabel F. Cruz
University of Illinois at Chicago
ifc@cs.uic.edu

We consider collaborative applications of wireless mobile devices where users (possibly from different organizations) are not previously identified, therefore the actions that they can perform are dynamically determined based on their own attribute values (e.g., location, acceleration, movement pattern, delegated credentials) and on the attribute values associated with computational (e.g., data, web services) or physical (e.g., hospital, army compound) resources. In what follows, we further detail some of the research issues and approaches.

Security Model. We extend the role-based access control (RBAC) model where roles are organized in a hierarchy. Also, in our model, users are not statically identified, therefore the actions that they can perform are determined based on the association between their own attribute values and the attribute values of the resources [1]. We perform a two-step matching of attribute values: of *actions* with resources (e.g., *enter* Air Force base) and of *users* with roles (e.g., *people with membership cards* are preferred museum guests) [2, 3].

Context-Aware Environments. In these environments, attribute values can vary over time (e.g., the user's location or whether the resource is open for visiting) thus enabling or disabling a user's ability to perform an action on a particular resource. A special but important case is the concept of being location-aware [5]. In this case, authorization decisions must be dynamically determined taking into account both organization-based user's roles and context-based attribute values that can vary over time depending on the user's location [4].

Collaborative Applications. A variety of situations may arise for collaborative applications. For example, each organization may have their own hierarchy of roles [3]. Also, there may exist a complex interplay among static and dynamic attribute values of users and resources [7]. The collaboration semantics as well as the particular access control models that will enact that semantics need to be determined.

Semantic Web Languages. In the above scenarios, it is necessary to model complex situations and to perform reasoning so as to determine at any instant the type of access of each user to each resource. Several considerations are at play including the expressiveness of the modeling languages and of the reasoning mechanisms, as well as their efficiency, so that such a framework can be used in real time. The expressiveness of semantic web languages has been studied to determine their adequacy to those scenarios [3, 6]. Furthermore, the development of system prototypes can provide important insight into this problem [4].

References

[1] M. A. Al-Kahtani and R. Sandhu. A Model for Attribute-Based User-Role Assignment. In *Annual Computer Security Applications Conference (ACSAC)*, pages 353–364. IEEE Computer Society, 2002.

[2] L. Cirio, I. F. Cruz, and R. Tamassia. A Role and Attribute Based Access Control System Using Semantic Web Technologies. In *International IFIP Workshop on Semantic Web and Web Semantics*, volume 4806 of *Lecture Notes in Computer Science*, pages 1256–1266. Springer, 2007.

[3] I. F. Cruz, R. Gjomemo, B. Lin, and M. Orsini. A Constraint and Attribute Based Security Framework for Dynamic Role Assignment in Collaborative Environments. In *International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom)*, pages 1–18. Springer, 2008.

[4] I. F. Cruz, R. Gjomemo, B. Lin, and M. Orsini. A Location Aware Role and Attribute Based Access Control System. In *ACM International Symposium on Advances in Geographic Information Systems (ACM GIS)*, pages 527–528, 2008.

[5] M. L. Damiani, E. Bertino, B. Catania, and P. Perlasca. GEO-RBAC: A Spatially Aware RBAC. *ACM Transactions on Information and System Security (TISSEC)*, 10(1):2, 2007.

[6] T. W. Finin, A. Joshi, L. Kagal, J. Niu, R. S. Sandhu, W. H. Winsborough, and B. M. Thuraisingham. ROWLBAC: Representing Role Based Access Control in OWL. In *ACM Symposium on Access Control Models and Technologies (SACMAT)*, pages 73–82, 2008.

[7] X. Zhang, M. Nakae, M. J. Covington, and R. Sandhu. A Usage-Based Authorization Framework for Collaborative Computing Systems. In *ACM Symposium on Access Control Models and Technologies (SACMAT)*, pages 180–189, 2006.