Security and Privacy in the Intelligent Environment

Rattapoom Tuchinda

Artificial Intelligence Laboratory
Massachusetts Institute of Technology
Cambridge, Massachusetts 02139

http://www.ai.mit.edu

The Problem: The idea of ubiquitous a computing environment where sensors and devices exist everywhere around us has opened up interesting security and privacy issues. Imagine a scenario in which Ben is working in an intelligent room. He does not want to be disturbed by anyone, so he tells the intelligent room that he does not want to be reached by anyone in the next two hours unless it is an emergency. The intelligent room satisfies Ben's request by asking a telephone agent to tell a caller that Ben is not here. It also asks a location agent not to reveal Ben's current location to anyone. After two hours have passed the intelligent room automatically revokes Ben's request.

The scenario above demonstrates that a ubiquitous computing environment needs an access control mechanism that is dynamic and service-based in addition to the traditional role-based access control.

Motivation: Security and privacy issues are usually ignored in many research topics because they make the system design more complicated. However, due to the pervasive nature of an intelligent environment, it is necessary to address these issues by establishing the framework for a security and privacy model.

Previous Work: Researches on an intelligent environment cover a wide area of topics [1]. Multimodal User Interfaces and Human-Computer Interaction are very popular, while device integration, system architecture, and networking begin to receive more attention. Security and privacy issues, however, are rarely addressed. Microsoft's Easy Living [3] asks users to authenticate themselves upon entering the room, however, it does not elaborate what kind of security model it has.

Implementing access control mechanisms into a system can solve some security and privacy issues. Role Based Access Control (RBAC) [5] is one of the most widely used access control in various industrail organizations such as banks [4] and hospitals [2]. However, no one has investigated RBAC in the context of the intelligent environment yet.

Approach: We started by investigating various real life scenarios and RBAC to see if RBAC is a practical access control to use in an intelligent environment such as the Intelligent Room at MIT AI Lab. The Intelligent Room is a shared space among many research groups and is used as a meeting room, dining room, and a movie room in some occasions. If RBAC can satisfy all scenarios in this shared space, multi-purpose intelligent room, then it will also work on a single purpose intelligent room such as a living room or a bedroom as these are just degenerated cases of the multi-purpose room.

The special characteristic of the Intelligent Room is that the room changes its function and users change their roles frequently. As a result, RBAC might be a good candidate for the Intelligent Room. However, there are at least three instances in which RBAC alone would not be practical.

- RBAC is strongly based on a notion of a role. A user takes on some roles. Based on those roles, the user will have access to some devices and information. Yet in some emergency situations, an access control should authorize the access based on a type of service that a user requests. For example, anybody should be able to tell the room to unlock the door if there is a fire.

- RBAC does not provide an easy framework to resolve a conflict when two or more users try to access the same resources. RBAC works well when used in database applications, because the chance of two users trying to access the same data is small. However, when two or more users are in the Intelligent Room, various resources such as lights and temperature control are shared among them.

- Dynamic rule generation and deletion like Ben's example in the problem section cannot be easily incorporated into RBAC.

Instead of trying to modify RBAC to address these problems, a new access control that is responsible for the three cases above can be implemented separately and work in parallel with RBAC. As a result, We design a security model that allows various access controls to be used. Each request for resources will be forward to each selected access control by an access control locators. The outcome of each access control can be combined to indicate whether the request is approved or not. This approach will allow a system administrator to combine advantageous features from each access control without having to modify a particular access control to make it work for all intelligent environments.

Impact: This research will provide the basis for the design of a security and privacy model in many intelligent environment settings such as schools, home, and workplaces. It offers a framework that allows a security administration to layout security policies and integrate information from new sensors. Moreover, security and privacy issues are the important factors that will determine whether the intelligent environment will be practical and commercializable or not.

Research Support: This work is funded by DARPA under contract number N66001-00-C-8078, administered by SPAWAR.

References:

[1]

[2] John Barkley. Application enginnering in health care. In *Second Annual CHIN Summit*, 1995.

[3] John Krumm Amanda Kern Brumitt Barry, Brian Meyers and Steven Shafer. Easyliving: Technologies for intelligent environment.

[4] Ramaswamy Chandramouli. Application of xml tools for enterprise-wide rbac implementation tasks. Technical report, National Institute of Standards and Technology, 2000.

[5] Kuhn Ferraiolo, Bugini. Role based access control: Features and motivations. In *Computer Security Applications Conference*.