

# Access Control in Smart Space Environments

Mike White  
TSSG, WIT  
<mailto:mwhite@tssg.org>

## Extended Abstract

Ubiquitous computing represents a departure from traditional computing environments where a predefined set of users interact within the confines of a closed network. The boundaries of both the network and the user set have expanded enormously. Traditional security approaches sought to address security issues in these restricted environments and tended to be identity based. This made sense as users within these environments shared a common goal and this tended to override the need for user privacy. Take for example the scenario of access to a network in a software development organisation, where everyone works towards a common goal e.g. develop a software product. It is not desirable or necessary for a user to anonymously produce code for some product. Because the network and user set are both well defined and restricted, it lends itself to traditional approaches but ubiquitous computing environments possess neither of these characteristics and as such requires a different security approach.

Traditional approaches have focused rigidly on the users' identity and how we can authenticate this identity. This more often than not took the form of checking whether the users' identity was contained in some white/black list local to the network concerned. This approach tended to preclude the effective implementation of solution that addressed two of the most important characteristics required of a security implementation in a ubiquitous computing environment, user defined privacy and scalability. Privacy concerns are accentuated by the fact that users within a smart space are not guaranteed to be local to the environment in which they are present. This raises questions regarding a smart spaces' access to a user's profile in order to garner enough

information in order to perform user authentication. A user will require that only attributes relevant to the actions he wishes to perform will be released.

As environments become more pervasive in nature the importance of adequate privacy protection is also heightened. Campbell et al [1] argue how the very same features that make pervasive computing environments convenient and powerful make them vulnerable to new security and privacy threats. Ubiquitous computing environments strive to leverage context information such as physical location in order to enhance user experience. But this improved user experience can give rise to certain undesirable consequences where a user's privacy is exploited against the users wishes. There is a real danger of smart spaces being used as a mechanism of unwarranted surveillance.

What is needed is less intrusive and more accurate forms of authentication. Take for example the user entering a public smart space and hoping to browse the services that are on offer to him/her. It is not necessary or desirable from a user perspective for a smart space to obtain a user's personal information in this circumstance. Support for anonymity is a likely requisite of any security approach adopted by a smart space. Only when a user's identity is necessitated by a requested action should a user's identity be released. Similarly take the example of the prepaid customer entering a smart space and wishing to avail of some service that incurs a charge. The identity of the customer and personal details such as his home billing address are not a relevant means of authentication but the user's possession of suitable attributes such as the of possession of a valid account with a valid prepaid account provider and the attribute of possessing sufficient credit to carry out a

required transaction are. Clarke [2] argues how the deployment of authentication without the disclosure of identity represents a real opportunity to unlock the potential of e-commerce an aspect of ubiquitous computing that is essential to its widespread adoption. Indeed authentication without identification is how our cash based monetary system is implemented and remains the most successful anonymity based commercial system available today.

The transient nature of certain smart space user sets exposes the smart space to greater security risks than those encountered by closed network environments. Access control policies for smart space environments must reflect a user set profile where users can be anonymous or have undertaken different levels of authentication. Indeed this greater security risk can be attributed in no small measure to the need for anonymity and the need to respect user's privacy as outlined in the preceding sections. An adaptive access control mechanism is required in order to deal with the changing user profile of certain smart space environments. If the presence of an anonymous or un-trusted users affects access control rights of other users in the smart space, all relevant access control rights should be updated accordingly. This principle can also be extended to allow a hierarchical approach to access control policies where access control rights can dynamically changes according to the hierarchical profile of the user set present in the smart space environment.

The necessity for a security solution to be scalable is accentuated by pervasive environments. Maintaining a white list of valid users is sufficient within a closed environment but in pervasive computing environments the boundaries of the user set is not so well defined. Take for example the scenario of an airport smart space; the number of potential users excludes the use of traditional authentication methods as used in a closed network environment. Atlanta's Hartfield-Jackson International Airport handled more than 79 million passengers in 2003 and gives some idea of the potential user base available to certain potential smart space environments [3]. A fragmented approach to the administration of such large user bases by individual smart spaces would prove both inefficient and difficult to maintain in a consistent manner. There are also drawbacks from a user's point of view; it is prohibitive for a user to maintain account information for each smart space he wishes to avail of and also it prevents a user from availing of certain

services contained in a smart space without a prior agreement.

This paper will outline the M-Zones Access Control Service (MACS). MACS is designed to provide an authentication and authorization service for an M-Zones environment [4]. The M-Zones programme is concerned with the management of smart spaces and as such any security solutions implemented should address the issues raised throughout this section concerning smart space environments.

## References

- [1] R Campbell, Jalal Al-Muhtadi, P Naldurg, G Samplemane, M Mickunas: Towards Security and Privacy for Pervasive Computing, Proceedings of the International Symposium on Software Security, Keio University, Tokyo, Japan, 2002
- [2] R Clarke, Authentication Re-visited: How Public Key Infrastructure Could Yet Prosper, <http://www.anu.edu.au/people/Roger.Clarke/EC/Bled03.html> : Visited May 2004
- [3] Airports Council International: <http://www.aci-na.org/>
- [4] M-Zones: <http://www.m-zones.org> : Visited May 2004