IRM PRESS
701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.irm-press.com
ITB10720

Chapter XV

Security in Pervasive Computing

Sajal K. Das, University of Texas at Arlington, USA

Afrand Agah, University of Texas at Arlington, USA

Mohan Kumar, University of Texas at Arlington, USA

Abstract

Security requirements for pervasive computing environments are different from those in fixed networks. This is due to the intensity and complexity of the communication between the user and the infrastructure, the mobility of the user, and dynamic sharing of limited resources. As pervasive computing makes information access and processing easily available for everyone from anywhere at anytime, the close relationship between distributed systems and mobile computing with a pervasive infrastructure leads us to take a closer look at different types of vulnerabilities and attacks in such environments. Pervasive computing includes numerous, often transparent, computing devices that are frequently mobile or embedded in the environment, and are connected to an increasingly ubiquitous network structure. For example, when an organization employs pervasive computing, the environment becomes more knowledgeable about the users' behavior and, hence, becomes more proactive with each individual user as time passes. Therefore, the user must be able to trust the environment and the environment must be confident of the user's identity. This implies security is an important concern in the success of pervasive computing environments. In this chapter we evaluate the suitability of existing security methods for pervasive environments.

This chapter appears in the book, *Wireless Information Highways,* edited by Dimitrios Katsaros, Alexandros Nanopoulos and Yannis Manalopoulos. Copyright © 2005, IRM Press, an imprint of Idea Group Inc. Copying or distributing in print or electronic forms without written permission of Idea Group Inc. is prohibited.

Introduction

Advances in technology provide isolated means for detecting and perhaps preventing security violations reactively. However, there is a need to glue these disparate technologies together so as to provide proactive infrastructure support and services for managing security-related issues. It is an extremely challenging task to process the information collected from sensory devices, interpret them meaningfully in the context of ongoing events, and accordingly carry out automated security services. This requires continual and proactive, real-time collaborations among physical devices, software agents, and personnel in dynamic, heterogeneous, autonomous environments.

The fundamental principles that guide pervasive computing environment design evolved from distributed systems. So in order to understand the concept of pervasive computing, we first begin describing the two closely related fields: distributed systems and mobile computing. As described in Satayanarayanan (2001), the following five areas are fundamental to distributed systems: (a) remote communication, (b) fault tolerance, (c) high availability, (d) remote information access, and (e) security. High bandwidth and low error rate in distributed systems make it possible to break down centralized software systems into separate network-connected components.

Although many basic principles of distributed systems are common to mobile computing as well, the following additional key features are fundamental to mobile computing: (a) unpredictable variation in wireless network communication quality, (b) lowered trust, (c) limitations on local resources, and (d) battery power consumption.

The ability to communicate remotely, access distributed files, share resources, and roam are the underlying challenges of a pervasive computing environment. In such an environment, if the nodes of the network are like agents that are programmable, or are able to move with the program and execute in different locations of the network, we would be able to have the benefits of active networks, which are thus essential components of pervasive computing infrastructures.

Many difficult design and implementation problems must be solved to realize pervasive computing. The main challenge we try to address in this chapter is security. Any successful pervasive computing environment uses smart spaces effectively and masks uneven conditions. Usages of smart spaces and masking uneven conditions have some degree of conflict when we embed the security aspects into them. Eavesdropping on wireless links is very easy, so the security of wireless communications can be easily compromised, especially if transmissions happen in a large area or while users are allowed to cross security domains, like giving permission to use one service in one environment but prohibiting the use of another service in the same area. Protecting the identity of the user, securing the information flowing between a user and base station, and achieving security and authentication are very hard tasks to do in a wireless environment. We study the existing security methods and discuss how to enhance them for pervasive computing.

To have a better feeling of life in a pervasive computing world, let us consider an example (Satayanarayanan, 2001). Suppose "Fred" is in his office and is preparing for his presentation in a meeting room, which is about a 10-minute walk across the campus. As he is not completely done with his presentation, he grabs his handheld computer. His files