Chapter 10
Secure and Private Service Discovery in Pervasive Computing Environments

Feng Zhu
University of Alabama in Huntsville, USA

Wei Zhu
Intergraph Co, USA

ABSTRACT

With the convergence of embedded computers and wireless communication, pervasive computing has become the inevitable future of computing. Every year, billions of computing devices are built. They are ubiquitously deployed and are gracefully integrated with people and their environments. Service discovery is an essential step for the devices to properly discover, configure, and communicate with each other. Authentication for pervasive service discovery is difficult. In this chapter, we introduce a user-centric service discovery model, called PrudentExposure, which automates authentication processes. It encodes hundreds of authentication messages in a novel code word form. Perhaps the most serious challenge for pervasive service discovery is the integration of computing devices with people. A critical privacy challenge can be expressed as a "chicken-and-egg problem": both users and service providers want the other parties to expose sensitive information first. We discuss how a progressive and probabilistic model can protect both users' and service providers' privacy.

INTRODUCTION

Every year, billions of computing devices are built and seamlessly integrated into our surroundings and daily lives. In the near future, we will live in pervasive computing environments. In these environments, devices range from traditional PCs, printers, or servers, to devices that people carry, wear, and to the devices that are embedded into commodities and ambient environments. Smart phones, iPods, smartcards, RFID tags, and various sensors are already ubiquitous. New types of devices are emerging rapidly. It is predicted that within a decade one may interact with thousands of computing devices in pervasive computing environments.

Unlike traditional computing environments, pervasive computing poses at least two new chal-

DOI: 10.4018/978-1-61520-783-1.ch010

lenges: a great number of devices and extremely dynamic computing environments. Unattended devices and service or partial failures may cause network services inaccessible. New networks services may be added and old services may be removed.

Service discovery is essential to address the two challenges in pervasive computing environments (Zhu, Mutka & Ni 2005). It enables devices and network services to properly discover, configure, and then communicate with each other via a network protocol. The protocol is called service discovery protocol. In next section, we provide more detailed explanation of service discovery protocols and discuss some representative protocols. These protocols greatly reduce the administrative overhead that users and system administrators have to conduct manually nowadays. Device driver installation and network service configuration are all automated by the protocols. Without service discovery protocols, administrative overhead for thousands of devices in one's vicinity is infeasible even for skilled system administrators in pervasive computing environments.

Moreover, service discovery protocols use soft states and lease-based service access to manage network services in the extremely dynamic pervasive computing environments. Soft state means that a service frequently updates its availability information. Lease-based service access allows a client device to access a service for a predetermined period of time. The client needs to renew the access request to further use the service. Both mechanisms gracefully handle failures of the unattended services and networks as well as service addition and removal.

Coupled with wireless networks, service discovery simplifies communication among devices and services. Without connecting cables and manually setting up devices or services, these devices and services can be discovered and configured automatically. Nevertheless, it creates three new security and privacy challenges.

First, computing environments are different. The boundaries are different. Physical boundaries may be disappeared. For example, at present, a digital camera in a bag is not accessible to others. But, if a digital camera communicates with other devices over wireless networks and runs a service discovery protocol, a stranger sits near the bag on a bus might be able to discover the digital camera and access its photos. As Ross Anderson points out, many security solutions failed because of the environments' change (Ross 2008).

Second, unlike relatively homogeneous computing environments in enterprises, in pervasive computing environments, multiple service providers may co-exist at a place. For instance, in Alice's office, the company provides network services. When Alice and her colleagues carry and wear devices and shares with each other, they become service providers. In addition, services provided by the city might also be accessible from her office. Ideally, secure and private service discovery should determine who has privileges to discover and access services. At the same time, service discovery should prevent unauthorized users to discover and access pervasive services even they are in the vicinity. Without proper protection, privacy may be sacrificed. For example, a malicious attacker may find the presence of a person by querying whether a handheld device is in the vicinity. Attackers may also query the devices and services that one carries or wears to find his or her preferences. If an attacker discovers a medical device that one wears, the patient's health information might be inferred.

Third, as we own more and more devices and become service providers, the relationships among users, devices, services, and service providers become more and more complex. Usability is a serious challenge. It is infeasible to require users to memorize all identities and associated passwords or certificates from various service providers. It is also overwhelming for users to memorize the relationship between services and service providers.