Chapter II
Secure Service Discovery

Sheikh I. Ahamed
Marquette University, USA

Munirul M. Haque
Marquette University, USA

John F. Buford
Avaya Labs, USA

Nilothpal Talukder
Marquette University, USA

Moushumi Sharmin
Marquette University, USA

ABSTRACT

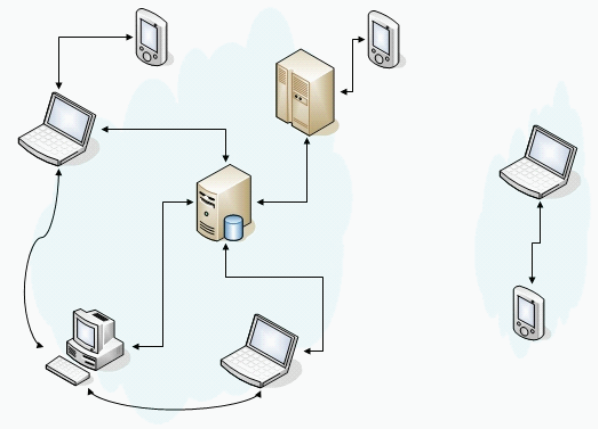
In broadband wireless networks, mobile devices will be equipped to directly share resources using service discovery mechanisms without relying upon centralized servers or infrastructure support. The network environment will frequently be ad hoc or will cross administrative boundaries. There are many challenges to enabling secure and private service discovery in these environments including the dynamic population of participants, the lack of a universal trust mechanism, and the limited capabilities of the devices. To ensure secure service discovery while addressing privacy issues, trust-based models are inevitable. We survey secure service discovery in the broadband wireless environment. We include case studies of two protocols that include a trust mechanism, and we summarize future research directions.

INTRODUCTION

Service orientation is widely used in client-server computing and is growing in importance for mobile wireless devices. In this way, a device's software and hardware components can be packaged as services for use by other devices. Many consumer electronics (CE) devices are specialized for specific uses. Due to form factor and cost considerations, devices vary in capability. With sufficiently high bandwidth network interfaces on these devices, such as 802.11, WiMax, and ultra-wideband (UWB), it is practical for sets of networked devices to share functionality. Service discovery and advertisement (SDA) is fundamental to service interoperability in pervasive computing applications.

Many service discovery protocols have been developed, including several for specific wireless networks. However, few of these protocols have been designed with security mechanisms and the majority use centralized enforcement and validation. Due to the emergence of mobile and large-scale peer-to-peer applications, there is growing

Figure 1. Different types of networks in a pervasive computing environment. (a) Ad hoc network in a pervasive environment with powerful device support. (b) Ad hoc network in a pervasive environment without powerful device support.



(a) *(b)*

interest in security mechanisms that do not require centralized enforcement and validation.

We present the current state of secure service discovery. Leading designs for secure service discovery are surveyed including industry standards and research systems. The types of security issues we are concerned with include: protecting the privacy of service advertisements and descriptions; authentication of service advertisements; secure distribution and updating of keys for service invocation; providing trust in service composition; and limiting vulnerability to attacks effecting the service discovery mechanism.

Pervasive computing environment focuses (Weiser, 1991, 1993) has evolved over the past few years with the availability of portable low-cost devices (such as PDAs, cell phones, smart phones, laptops, and sensors) and the emergence of short-range and low-power wireless communication networks. Pervasive computing environments focus on integrating computing and communications with the surrounding physical environment to make computing and communication transparent to the users in everyday contexts. In a broad sense, pervasive computing combines mobile computing, wireless networks, embedded computing, and context-aware sensor networks (Robinson, Vogt, & Wagealla, 2005).

The different kinds of networks in pervasive computing environments impact the design of secure service discovery mechanisms. On one end, there are smart spaces, or intelligent environments that provide devices with a variety of support for user awareness and context management, while at the other end there are networks that provide open network connectivity.

Figure 1 depicts two ad hoc networks in a pervasive computing environment. In Figure 1a, the devices communicate among themselves with the support of fixed, more powerful devices. These devices act as servers or proxies for the mobile devices. In Figure 1b, an ad hoc network is formed by mobile devices. There is no fixed infrastructure support. The devices communicate with each other directly or via another mobile device, and are responsible for performing computations by themselves.

In service discovery (Kindberg & Fox, 2002; Lee & Helal, 2002), a device searches for another device capable of offering a specific service or resource. An important trend is the adoption of a service-oriented architecture for resource discovery, not just for server systems accessed by