Chapter X
Security Issues in Pervasive Computing

Lawan Ahmed Mohammed
King Fahd University of Petroleum and Minerals, HBCC Campus, Saudi Arabia

Kashif Munir
King Fahd University of Petroleum and Minerals, HBCC Campus, Saudi Arabia

ABSTRACT

The change in physical structures of computing facilities into small and portable devices, or even wearable computers, has enhanced ubiquitous information processing. The basic paradigm of such pervasive computing is the combination of strongly decentralized and distributed computing with the help of diversified devices allowing for spontaneous connectivity via the Internet. In general, pervasive computing strives to simplify day-to-day life by providing mobile users with the means to carry out personal and business tasks via mobile and portable devices. This chapter examines the security challenges that are barriers to mainstream pervasive computing and explains why traditional security mechanisms fail to meet the demands of these environments.

INTRODUCTION

Computing today is moving away from the desktop and becoming diffused into our surroundings as wearable, portable and movable devices such as laptop, smartphone, pager, mobile phone, PDA, and the like. This new trend in computing is known as *pervasive computing*. The new trend describes an environment where a wide range of devices carry out information processing tasks on behalf of users by utilizing connectivity to wide variety of networks. Pervasive computing does not just mean “computers everywhere”; it means “computers, networks, applications, and services everywhere.” It is concerned with the way people view mobile computing devices, and uses them within their environments to perform tasks. It deals with the way applications are created and deployed to enable such tasks to be performed. The realization of this computing paradigm is not far fetched. An average person today already owns vast numbers of consumer devices, electronic gadgets, and gizmos that already have processors, microcontrollers, and memory chips embedded into them. Today, mobile phone handsets are arguably the dominant computer form factor consumers’ purchase. These devices have become powerful and sophisticated, many are even more powerful than desktop computers of the late 1990s (David et. al., 2004). They are capable of receiving TV and cable network services, radio station services and other audio-visual services in addition to communication services. The vehicles we use on daily basis already have a large number of embedded computers handling different subsystems of the vehicle, like ABS (Anti-lock Braking System) and ESP (Electronic Stability Program). Technologies like Bluetooth and Wi-Fi make it possible to embed networking capabilities into any small devices without hassle (Roy et. al., 2002). In effect, these technologies help make networking much more general and achievable even on elementary devices, like toasters and paperclips. In such computing environments, these services will increase both the complexity of information infrastructures and the networks which support them. However, Information stored, processed, and transmitted by the various devices is one of the most critical resources. Threats exploiting vulnerabilities of new kinds of user interfaces, displays, operating systems, networks, and wireless communications will cause new risks of losing confidentiality, integrity, and availability.

In this chapter we organize and present various security challenges associated with the pervasive computing and also proposed some countermeasures. In particular, we look at three different entities (the device, the network, and the users) involved in the system and outline the security requirements that are related to each specific entity. Other objects such as mobility, wired and wireless communication, and secure hardware/software platforms are also briefly discussed. The main objective of the chapter is to highlight and clarify the security issues and problems in pervasive computing environment that need to be addressed by the research community.

SECURITY CHALLENGES IN PERVASIVE COMPUTING ENVIRONMENT

Pervasive computing environment or PCE share most of the security issues of traditional networked applications. These include authentication of devices and users, privacy of data or information, defense against malicious code such as viruses, worms, Trojan horses etc, and access control mechanisms. However, the pervasive computing environment adds some unique issues to the already complex security arena. Physical security is important as the devices can be easily misplaced or stolen. Information that is usually confined behind a corporate firewall is now winging its way through the air, possibly spending some time on hosted servers or wireless gateways. The challenges of securing ubiquitous society environment are illustrated in Figure 1 (Chan et al., 2004)

The techniques of hacking mobile devices such as laptops, cell phones, PDAs etc is already spreading. In view of these, adding security to such environment presents challenges at different levels. For instance, having a central authority for a single building or even a group of rooms is infeasible because every possible access right will have to be specified for every user. Authenticating the identity certificate of a previously unknown user