Chapter 13
A Novel Intrusion Detection System for Smart Space

Bo Zhou
Liverpool John Moores University, UK

Qi Shi
Liverpool John Moores University, UK

Madjid Merabti
Liverpool John Moores University, UK

ABSTRACT

An Intrusion Detection System (IDS) is a tool used to protect computer resources against malicious activities. Existing IDSs have several weaknesses that hinder their direct application to ubiquitous computing environments like smart home/office. These shortcomings are caused by their lack of considerations about the heterogeneity, flexibility and resource constraints of ubiquitous networks. Thus the evolution towards ubiquitous computing demands a new generation of resource-efficient IDSs to provide sufficient protections against malicious activities. In this chapter we proposed a Service-oriented and User-centric Intrusion Detection System (SUIDS) for ubiquitous networks. SUIDS keeps the special requirements of ubiquitous computing in mind throughout its design and implementation. It sets a new direction for future research and development.

1. INTRODUCTION

With the wide spread of computers, our daily lives are highly computerised and closely connected with computer networks. In the near future, one will be able to open a door by simply sending an order to the electric door lock from his/her PDA, or read news on a computer embedded "e-paper" with the content updated through wireless connections. The trend towards a computerised smart space is part of the conception of *ubiquitous computing* (Weiser 1991). In the era of ubiquitous computing, devices with computing and communicating abilities will surround us all over. Eventually it will achieve the non-intrusive availability of computers throughout physical environments.

DOI: 10.4018/978-1-60566-836-9.ch013

Just like other networks, one of the main prerequisites for a ubiquitous network is adequate security (Stajano 2002). The network has to be properly secured so that it can be relied upon. On the one hand, people want to construct a ubiquitous network to make the best use of computers; on the other hand, they must secure their network in order to cope with a number of security threats from malicious entities.

Intrusion Detection Systems (Axelsson 2000; Sabahi 2008) are widely used to protect computer networks. If an intrusion is detected quickly enough, the intruder can be identified and ejected from the system before any damage is done or any data are compromised. Moreover, an effective intrusion detection system can even serve as a deterrent, acting to prevent intrusions.

Traditional IDSs, which were originally developed for wired networks, are not suitable for ubiquitous computing due to the unique characteristics and inherent vulnerabilities of the environment. This unfitness directly compromises the effectiveness and efficiency of existing IDSs. For example, with the concept of ubiquitous computing, there must be some small-size devices in order to achieve unaware deployment. Inevitably, they will have limited energy supplies and storage spaces. An obvious issue is how to implement an IDS in a resource-effective way. This is a big challenge since one of the most desirable features for an IDS is real-time detection and response, which is extremely energy consuming. Another key issue is related to the system architecture. Current host-based IDSs do not fit for ubiquitous computing due to the nodes' capacity constraints, while network-based IDSs simply cannot capture inside users' activities as the network's infrastructure tends to be heterogeneous.

The above discussion indicates that the evolution towards ubiquitous computing demands a new generation of resource-efficient IDSs to provide sufficient protections against malicious activities. The aim of this chapter is to analyse the requirements on such an IDS and propose a suitable solution. It should have an appropriate system architecture and detection strategy to be flexible and energy-efficient.

The objectives of this chapter are:

- To provide a background to ubiquitous computing and demonstrate the unfitness of existing IDSs when applying them to ubiquitous computing environments.
- To posit the requirements for an appropriate IDS that is associated with resource-sensitive design and distributed modules' deployment.
- To present the design of a system (i.e. SUIDS, standing for Service-oriented and User-centric Intrusion Detection System) that detects security attacks at the service layer and builds a defence wall against malicious users.
- To prototype the SUIDS system in order to provide proof-of-concept for proposed work and perform an assessment in relation to the proposed requirements, where possible.
- To propose an original set of mechanisms, strategies and protocols that together achieve energy-efficiency in SUIDS.

2. BACKGROUND

2.1 Ubiquitous Computing

The term of *ubiquitous computing* was first mentioned in Mark Weiser's article "The Computer for the 21st century" (Weiser 1991). The author explained that the most powerful and successful technologies are