Chapter 30
The Context–Security Nexus in Ubiquitous Computing

M. Fahim Ferdous Khan
The University of Tokyo, Japan

Ken Sakamura
The University of Tokyo, Japan

ABSTRACT

Context-awareness is a quintessential feature of ubiquitous computing. Contextual information not only facilitates improved applications, but can also become significant security parameters – which in turn can potentially ensure service delivery not to anyone anytime anywhere, but to the right person at the right time and place. Specially, in determining access control to resources, contextual information can play an important role. Access control models, as studied in traditional computing security, however, have no notion of context-awareness; and the recent works in the nascent field of context-aware access control predominantly focus on spatio-temporal contexts, disregarding a host of other pertinent contexts. In this paper, with a view to exploring the relationship of access control and context-awareness in ubiquitous computing, the authors propose a comprehensive context-aware access control model for ubiquitous healthcare services. They explain the design, implementation and evaluation of the proposed model in detail. They chose healthcare as a representative application domain because healthcare systems pose an array of non-trivial context-sensitive access control requirements, many of which are directly or indirectly applicable to other context-aware ubiquitous computing applications.

INTRODUCTION

The fact that ubiquitous computing represents the latest paradigm shift in computing necessitates a paradigm shift in how security is addressed in conventional computing. This paradigm shift in computing security – as believed by many researchers – can effectively be achieved by making security context-aware. Context-awareness is the essence of ubiquitous computing (Koshizuka & Sakamura, 2010), so much so that it is often dubbed as context-aware computing. Moreover, the relation between security and context is rather intuitive: what is secure in one context may not be secure in other contexts. Recognizing the notion of context as an important denominator of both

DOI: 10.4018/978-1-4666-9624-2.ch030

ubiquitous computing and security, this paper aims at exploring the relationship of security and context-awareness in ubiquitous computing.

The notion of context has been observed in numerous areas, including linguistics, philosophy, knowledge representation and problem solving in the field of artificial intelligence, and the theory of communication. Dey (2001) gives an operational definition of context, which arguably turns out to be very useful in practice and suitable for ubiquitous computing: "Context is any information that can be used to characterize the situation of an entity. An entity is a person, place, or object that is considered relevant to the interaction between a user and an application, including the user and applications themselves." There has been much work in identifying what such information can be, the structure of the information, how to represent such information, and how to exploit context in specific applications. Contexts can include information such as location (e.g., of people or objects), time, execution state of applications, computational resources, network bandwidth, activity, user intentions, user emotions, and conditions of the environment (Schmidt, Beigl & Gellersen, 1999).

Traditional security models help to ensure integrity, nonrepudiation, and confidentiality of information. Security seems inherently contextual and relative to the environment and circumstances; what is secure in one situation is considered insecure in another; information is insecure if it is viewed not by the right people, not at the right time, and not in the right circumstances. With mobile and ubiquitous computing developments, information can be accessed in more ways and in more places than ever before and in forms not previously possible. Moreover, the context in which such information is viewed or used can change given the agility and mobility made possible by new devices and wireless networking technologies. Also, advancement in sensing technologies have narrowed the gap between the physical and virtual world, so that the computer can have a better picture of the physical world via advanced, and increasingly widespread, sensor technology and sensor information processing techniques. With computers having the ability to acquire context information of people and things and recognize situations, the opportunity becomes available for computers to help manage secure information with its own better knowledge of the physical world. Context-awareness can help provide fine-grained and more appropriate security as identity authentication can be combined with various contextual information that validate or invalidate access to the pertaining resources. Let us give some simple examples based on obvious contexts of location and time. In an online examination, the student should be able to access the question paper only when s/he is in the exam hall on the prescribed date and time. Relying on only user name and password would not suffice in this case. In healthcare scenario, a doctor should be able to access patient information only during working hours from the hospital. In a military setting, a missile can be launched only in physical presence of authorized military staff while the missile is in a secure missile base. In short, as ubiquitous computing enables omnipresence of connectivity and information, any access to resource or transaction must be validated against pertinent spatio-temporal restrictions. However, location and time are not the only contexts (Schmidt et al., 1999); there are other important contexts, as we will see in section 3, that are important in determining access decisions.

In this article, we endeavor to explore the strong correlation between access control and context-awareness, taking healthcare system as an example. Our choice of healthcare system was motivated by the rich contexts that are such a system presents. We argue that many of these contexts are congruent to other context-aware ubiquitous computing applications. In particular, we present a context-aware access control model for healthcare informatics. The rest of this paper is organized as follows. The second section presents