Chapter 2.11
A Game Theoretic Approach to Optimize Identity Exposure in Pervasive Computing Environments

Feng Zhu
The University of Alabama in Huntsville, USA

Sandra Carpenter
The University of Alabama in Huntsville, USA

Wei Zhu
Intergraph Co., USA

Matt W. Mutka
Michigan State University, USA

ABSTRACT

In pervasive computing environments, personal information is typically expressed in digital forms. Daily activities and personal preferences with regard to pervasive computing applications are easily associated with personal identities. Privacy protection is a serious challenge. The fundamental problem is the lack of a mechanism to help people expose appropriate amounts of their identity information when accessing pervasive computing applications. In this paper, the authors propose the Hierarchical Identity model, which enables the expression of one's identity information ranging from precise detail to vague identity information. The authors model privacy exposure as an extensive game. By finding subgame perfect equilibria in the game, the approach achieves optimal exposure. It finds the most general identity information that a user should expose and which the service provider would accept. The authors' experiments show that their models can reduce unnecessary identity exposure effectively.

DOI: 10.4018/978-1-61350-323-2.ch2.11

INTRODUCTION

We expose personal information frequently in our daily tasks. Often, we unnecessarily expose too much information. For example, Bob proves that he is an adult by using his driver's license. At the same time, he unnecessarily exposes his driver's license number, birth date, name, home address, sex, eye color, hair color, and height. Different amounts of exposure may have dramatic differences in sensitivity. If Bob just proves that he is older than a certain age, the verifying party only knows that he is one of billions of adults. In contrast, his driver's license information uniquely identifies him in the world. In pervasive computing environments, we interact with intelligent ambient environments. Much more personal information is expressed in digital forms, is communicated over networks, and is permanently stored. Multiple types of ID cards such as employee IDs, driver's licenses, passports, and credit cards are already using embedded processors and can communicate over wireless networks. Proper identity exposure becomes more critical to protect our privacy because identities are associated with our daily activities, preferences, context, and other sensitive information. Without privacy protection, pervasive computing may become a distributed surveillance system (Campbell, Al-Muhtadi et al., 2002).

Exposing the appropriate amount of personal identity information to the appropriate parties is challenging. First, we may have many types of identities associated with our different life roles. To access pervasive services, with which we may or may not be familiar, a variety of identity elements need to be exposed. Second, users may not be able to make rational exposure choices. Many people's privacy awareness is very limited. For example, people carelessly provide their detailed personal information on the Internet (Dyson, 2006). Third, unnecessary exposure may be lured, requested, and forced. Stores give discounts to customers who provide their personal information. At the checkout register, customers are often asked for their home phone numbers, by which their home addresses and names can be found. According to the Georgetown Study of 361 randomly selected U.S. commercial websites with a minimum of 32,000 unique visitors in a month, the common practice is that almost all service providers (more than 90%) collected various identity information (Culnan, 2000). Data show that service providers extensively use identity information (NativeForest.org, 2009). Some may even aggressively sell their customers' identity information (Gellman, 2002).

The laws and regulations that protect privacy provide protection only on data usage (Langheinrich, 2001). Privacy exposure is often left up to an individual's decision. Once personal information is unnecessarily exposed, it is out of a user's control. Langheinrich suggests that privacy should be built into in pervasive computing systems because law makers and sociologists are still addressing yesterday's and today's information privacy issues (Langheinrich, 2001).

Anonymity is an approach to prevent identity exposure (Chaum, 1981, 1985; Campbell, Al-Muhtadi et al., 2002; Beresford & Stajano, 2003; Gruteser & Grunwald, 2003). It hides users' identities such that a user is not discernible from other users. Anonymity protects privacy by hiding the identity information, but sometimes exposure is necessary. A critical issue is the appropriate exposure: whether the requested identity information should be exposed and what identity information should be exposed. Several research works use policy-based approaches (Leonhardt & Magee, 1998; Snekkenes, 2001; Langheinrich, 2002; Hong & Landay, 2004), such that users' personal information is not exposed unless service providers' policies meet users' preferences and policies. The systems require users to have the special skills required to specify policies. But users might still sacrifice their privacy for convenient service access.