Chapter 101
Is It Privacy or Is It Access Control?

Sylvia L. Osborn
The University of Western Ontario, Canada

ABSTRACT

With the widespread use of online systems, there is an increasing focus on maintaining the privacy of individuals and information about them. This is often referred to as a need for privacy protection. The author briefly examines definitions of privacy in this context, roughly delineating between keeping facts private and statistical privacy that deals with what can be inferred from data sets. Many of the mechanisms used to implement what is commonly thought of as access control are the same ones used to protect privacy. This chapter explores when this is not the case and, in general, the interplay between privacy and access control on the one hand and, on the other hand, the separation of these models from mechanisms for their implementation.

INTRODUCTION

The right to privacy is enshrined in international and national covenants and charters on human rights. Concern for the privacy of on-line data began with the introduction of computing systems. By 1980 the OECD published its guidelines dealing with the privacy of information and trans-border flow of information, OECD (1980). In the database community, the Hippocratic database paper, by Agrawal, et al. (2002), is considered the seminal paper in introducing privacy concerns to the database community. Meanwhile, access control has always been a part of computer systems.

We begin by examining definitions and dimensions of privacy preservation, continue with an introduction to Sandhu's OM-AM framework, consider the available mechanisms for implementing access-related models, and then comment on how all these ideas t together. We also briefly discuss the user. Our hope is that if there are gaps in the effective protection of information, this analysis might help to show where the gaps are.

DOI: 10.4018/978-1-5225-7113-1.ch101

PRIVACY VS. ACCESS CONTROL IN COMPUTER SYSTEMS

In this section, we review some definitions of access control and privacy, in order to crystalize their similarities and differences. Because the discussion of access control is shorter, we proceed with it first, followed by some definitions of privacy, and finally highlight their similarities and differences.

Access Control

Access control deals with controlling who has what kind of access to various resources. The resources can be physical (that is a computer system) or strictly deal with data. The data can describe documents, inventory, shipping requisitions for a large company, allocation of university courses to classrooms, the destination of an aircraft carrier, etc. In other words, although a lot of data concerns individuals, there is also a lot of other data dealing with other things. There are three well-known access control models. In the first, Discretionary Access Control (DAC), data is owned by the individual computer user (e.g. personal files in Unix); in Mandatory Access Control (MAC), control is centralized and it is assumed that the enterprise owns (and labels) all the data. The third is Role-based Access Control (RBAC), where permissions are grouped into roles and roles are assigned as a unit to users. RBAC has been shown to be able to simulate both MAC and DAC, Osborn, Sandhu, & Munawer, (2000).

The basic components of an RBAC system are users (U) or subjects, permissions (P) which are pairs (o, a) where "o" represents an object to be protected and "a", an access mode on this object. Roles (R) consist of a set of permissions, represented by a permission-role assignment (PRA). Users' membership in roles is represented by a user-role assignment (URA). Roles can be arranged in a hierarchy such that a senior role inherits the permissions of its junior(s), and members of a senior role are also members of its juniors.

Privacy

Privacy, on the other hand, typically infers that the data in question relates to human beings, or possibly to corporations. It is related to the right to privacy which is enshrined in international and national covenants and charters on human rights. The Merriam-Webster dictionary defines privacy as "freedom from unauthorized intrusion" (Web, 2014). The classic version of the Hippocratic oath contains the following[1]:

What I may see or hear in the course of the treatment or even outside of the treatment in regard to the life of men, which on no account one must spread abroad, I will keep to myself, holding such things shameful to be spoken about.

A definition given in a previous ISSA paper by Renaud, & Galvez-Cruz, (2010) is:

Privacy is the faculty and right that a person has to dene, preserve and control the boundaries that limit the extent to which the rest of society can interact with or intrude upon. At the same time, he or she retains full control over information generated by, and related to, him or her.