Chapter 100
Privacy Aware Access Control: A Literature Survey and Novel Framework

Rekha Bhatia
Punjabi University Regional Centre, India

Manpreet Singh Gujral
Chandigarh College of Engineering and Technology, India

ABSTRACT

Due to the ever increasing number of web services available through the Internet, the privacy as a fundamental human right is endangered. Informed consent and collection of information are two important aspects while interacting on the Internet through web services. The ease of data access and the ready availability of it through Internet, made it easier for interested parties to intrude into the individual's privacy in unprecedented ways. The regulatory and technical solutions adopted to curb this have achieved only a limited success. The main culprits in this regard are the incompatibilities in the regulatory measures and standards. This research work focuses on privacy preserving access control for sharing sensitive information in the arena of web services, provides some recent outlooks towards the critical need of privacy aware access control technologies and a comprehensive review of the existing work in this arena. Besides, a novel framework for privacy aware access to web services is also provided.

INTRODUCTION

There are several challenges posed by web services for keeping personal information private. The reason behind this is the open nature of web and web services which make it easier to share information among databases and applications. This ease of web is giving rise to privacy invasion and violations. In the early stage of web services development, these were independent, wholly providing services all alone. These services require clients to enter their sensitive personal information in order to have access to the service which needs privacy protection issues to be considered. These days, web services tend to collaborate with other existing services in order to serve the client's request thus composing new services on the fly. Privacy, in this scenario, has become much more important due to the increasing popularity of user data being collected, stored and shared through these service compositions. The goal of privacy

DOI: 10.4018/978-1-5225-7113-1.ch100

aware access control is to automate privacy management for providing better compliance to the needs of the service provider and service requester and ensure that personal data is accessed not only based on security policies but also on privacy policies.

Using Platform for Privacy Preferences (P3P) privacy policy language (Franke, 2001) user's privacy preferences can be compared automatically with the service privacy policies so that the users can decide whether to use that service or refrain from it. In case it matches and the user decides to use the service by providing his personally identifiable information (PII), then after he has used the service, the actual enforcement on PII usage of web services can be achieved through access control systems. An access control system's response to an access request is managed according to the access control policies written in a special access control language like Extensible Access Control Mark Up Language (XACML) ("OASIS eXtensible Access Control") which is the most widely used policy language for access control (Godik & Moses, 2002).

The composition of unknown heterogeneous web services from a single service to the merging of multiple services impacts the access control process greatly as P3P was designed from a single service viewpoint. For instance, its recipient element cannot express potential services that will be participating to form a composite service. Secondly, in the composed services, matching of user's privacy preferences with privacy policies of all the services, become cumbersome for P3P to handle in an efficient way. It is thus desirable to have a composite privacy policy so that the access decision can be taken automatically according to user's privacy preferences. However, there is no mechanism provided in P3P to prepare the privacy policy of the composite services. Another challenge, faced in P3P, is that it does not provide any mechanism for conflict resolution among various services' privacy policies.

This paper, firstly, provides a comprehensive literature survey of online privacy, privacy breaches on the Internet and privacy aware access control. Secondly, a novel privacy aware access control framework is proposed in this paper which will ensure that personal information is accessed by two or more communicating parties if agreed privacy policies and preferences are satisfied. We suggest the use of Hippocratic databases to store privacy preferences of the users and automatically match these preferences with the participating services to be suitable for composite web services. The Hippocratic database technology is being developed by IBM Research (Grandison, Johnson & Kiernan, 2008). The name of these databases has been coined from the Hippocratic Oath of doctors in which they pledge to keep the information about their patients as a secret from outsiders. These databases were first introduced by (Agrawal, Kiernan, Srikant et al., 2002) to incorporate privacy preservation in conventional relational database systems. The Hippocratic databases negotiate the privacy of information between a user and an organization. Before data is collected, the types of information to be obtained and basic rules about how the data will be used are decided. These rules include who should have access to the data and how long it will be retained. When a user enters information, an application at the user end will interact with the database to check that its data privacy policies are acceptable to the user, who has already programmed his or her preferences into the application. Once verified, data is transferred from the user to the database.

PRIVACY AND THE INTERNET

Informed consent and collection of information are two important aspects while interacting on the Internet. The ease of data access and the ready availability of it through Internet made it easier for interested parties to intrude into the individuals' privacy in unprecedented ways. Even all the technical