Chapter 9

Privacy Aware Systems: From Models to Patterns

Alberto Coen-Porisini
Università degli studi dell’Insubria, Italy

Pietro Colombo
Università degli studi dell’Insubria, Italy

Sabrina Sicari
Università degli studi dell’Insubria, Italy

ABSTRACT

Enterprises have adopted various strategies to protect customers’ privacy and to make public their policies. This chapter presents a conceptual model for supporting the definition of privacy policies. The model, described by means of UML, introduces a set of concepts concerning privacy and defines the existent relationships among those concepts along with the interfaces for the definition of privacy related mechanisms. The chapter also illustrates how the conceptual model can be used to build design solutions for three recurrent requirements for privacy aware systems concerning the definition of anonymity, the acquisition of the informed consent, and privacy policies enforcement. The proposed problems are separately illustrated and a solution based on the conceptual model is described for each of them. Finally, in order to assess the model and the design solutions, this chapter presents an example concerning the health domain.

INTRODUCTION

Nowadays privacy is a key issue and has received increasing attention from consumers, companies, researchers and legislators. Legislative acts, such as the European Union Directive\(^1\) for personal data, the Health Insurance Portability and Accountability Act\(^2\) for healthcare and the Gramm Leach Bliley Act\(^3\) for financial institutions, require governments and enterprises to protect the privacy of their citizens and customers, respectively. Although enterprises have adopted various strategies to protect customers privacy and to make public their privacy policies (e.g., publishing a privacy policy on web-sites possibly based on P3P\(^4\)), none of these approaches include systematic mechanisms to describe how personal data are actually handled after they are collected.

This chapter proposes a conceptual model that provides a sound foundation for the definition of
privacy policies. The model, which extends the work proposed by Coen-Porisini & al. (2007), is defined using UML\textsuperscript{5} and represents a general schema that can be easily adopted in different contexts.

A privacy policy defines the way in which data referring to individuals can be collected, processed and diffused according to the rights that individuals are entitled to. Thus, the model introduces the concepts, such as users, data, actions, that are needed in order to define a privacy policy along with the existing relationships among them.

Although the model introduces all the elements that are required for the definition of privacy aware systems, it operates at a conceptual level with a very high level of abstraction. The main benefit of this approach is represented by the fact that the model is domain independent and it can be used in different contexts. In this way analysts and designers can describe privacy related features/requirements and then they can integrate them at design time in new or existing systems exploiting the visibility and usability of UML.

In addition to presenting the above mentioned model, this chapter introduces a design solution to some privacy related requirements that are common to most privacy aware systems. The way in which such design solutions are provided is by means of design patterns (Gamma et al. 1994), which constitute a set of design guidelines and schemes that can drive the designer towards the specification of a privacy aware system.

In this chapter, for space reasons, we focus on the following three requirements: anonymity, informed consent acquisition and privacy policy enforcement. Notice that other privacy related requirements such as pseudonymity, unobservability and so on can be addressed in the same way by developing appropriate design patterns.

Anonymity is an important requirement for a privacy aware system that aims at protecting the identity of the individuals whose data are handled by the system. In general, data can be categorized into different classes. Among them, one class includes data, referred to as sensitive data, concerning the private life, political or religious creed and so on, while another class contains data that describes the identity of individuals (e.g., first name, family name, etc.). A privacy aware system must assure that only authorized users can view the existing relationship between sensitive data and the identity of the individuals.

Informed consent is another important requirement for privacy aware systems that aims at assuring individuals that the system will use their data according to their will. For instance many legislations require that individuals must be informed of both the reasons for which the system will handle their data and the way in which data processing is performed. In such cases every individual has to provide an explicit consent before any data processing can occur.

Privacy policies enforcement requires that the activities performed within a system are checked against the privacy policy in order to avoid any privacy violation.

Finally, in order to test the effectiveness of the conceptual model and of the proposed design solutions, we discuss their application by means of an example concerning the healthcare domain.

In the last few years, hospitals, clinics, surgeries, and diagnostic centers have increasingly adopted Information Technology-supported healthcare solutions in order to manage health-related information and to provide a (semi)automated administration of clinical functions. As a consequence, due to its critical nature, the healthcare domain represents an ideal field for experimenting the definition of privacy mechanisms.

The rest of the chapter is organized in the following way: Section 2 provides an overview of the main related works concerning privacy; Section 3 introduces the privacy model and discusses its main features; Section 4 illustrates how the proposed model can be used for defining design solutions that achieve specific requirements such as the anonymity, the informed consent and the enforcement of privacy policies; Section 5 presents
Related Content

A Semantic Approach to Deploying Product-Service Systems
[www.igi-global.com/article/a-semantic-approach-to-deploying-product-service-systems/197431?camid=4v1a](www.igi-global.com/article/a-semantic-approach-to-deploying-product-service-systems/197431?camid=4v1a)

Design of a Power Aware Systolic Array based Support Vector Machine Classifier
[www.igi-global.com/chapter/design-of-a-power-aware-systolic-array-based-support-vector-machine-classifier/135882?camid=4v1a](www.igi-global.com/chapter/design-of-a-power-aware-systolic-array-based-support-vector-machine-classifier/135882?camid=4v1a)

Adaptive Future Internet Applications: Opportunities and Challenges for Adaptive Web Services Technology
[www.igi-global.com/chapter/adaptive-future-internet-applications/188271?camid=4v1a](www.igi-global.com/chapter/adaptive-future-internet-applications/188271?camid=4v1a)

Execution Management for Mobile Service-Oriented Environments
[www.igi-global.com/article execution-management-mobile-service-oriented/47037?camid=4v1a](www.igi-global.com/article execution-management-mobile-service-oriented/47037?camid=4v1a)