Abstract

Usage control is concerned with what happens to data once the data have been released to a data consumer who is, in principle, able to use the data in any imaginable way. Considerations relating to privacy, intellectual property, and public security, however, suggest that data providers are often interested in imposing a certain amount of control on the data that they release. In the DUKE project, we address the problem how the usage of data can be controlled once the data have been given away.

1. Introduction

Access control governs who may access which data. Usage control governs also what may happen with the data after the data have been given away; thus it extends access control into the future. We study usage control in a distributed setting where the involved subjects can take on the roles of data providers (who give data away) and data consumers (who request and receive data). When a data provider gives data to a data consumer, the latter must adhere to certain conditions on the usage of the received data. The fact that data providers usually have no or little control over the data consumer makes the enforcement of usage control requirements a difficult problem.

Usage control is not only relevant in the areas of privacy and intellectual property management but also in mobile communication. The involved parties are the end users and their mobile devices, the network operator, and third-party service providers.

2. Contributions

In terms of specifying requirements on data usage, we developed the Obligation Specification Language (OSL) within DUKE. OSL is a general-purpose language for usage control policies. OSL is complemented by translation schemes between different policy languages and OSL. These schemes can enhance the interoperability of existing technologies and allow us to re-use special purpose mechanisms for enforcing OSL policies. For example, we can use DRM mechanisms for privacy enforcement.

Based on a survey of existing enforcement mechanisms, we defined a taxonomy for usage control enforcement mechanisms. We also specified a system model for data consumers and enforcement mechanisms that can be used for analysis purposes (e.g., whether a policy can be enforced with a given set of mechanisms) and for the configuration of enforcement mechanisms.

Further, we defined a generic architecture for data providers. One component of this architecture, which we prototypically implemented, is a monitor that observes whether certain obligations are fulfilled and, if this is not the case, can impose penalties on the data consumer. This enforcement strategy is useful if the data consumer does not allow the data provider to directly interfere with its information processing.

3. Future Work

Future work includes the propagation of policies and rights. This involves the questions of how policies must change when data are distributed further and how policies must change when data are processed or aggregated. Furthermore, we need methods of mapping abstract specifications of actions to commands on concrete systems, and the interoperability of policies and mechanisms needs to be further improved. An additional topic of future work is the negotiation of policies and enforcement mechanisms between data provider and data consumer and the usability of policies and mechanisms.

We as well plan to prototypically implement and evaluate the developed techniques.