ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Semester Thesis for Florian Schütz

Taxonomy of Control Mechanisms

Supervisors: Manuel Hilty, Alexander Pretschner
Professor: Prof. D. Basin
Issue Date: March 20th 2006

1 Introduction

How digital data may be used and distributed is a concern in many areas of information security. Data protection is about controlling the use of sensitive personal data to protect people's privacy. In digital rights management (DRM), usage of data is controlled in order to protect intellectual property rights. The use of confidential business or military data often needs to be controlled as well. Embracing all these areas, we define usage control (UC) as an extension of access control (AC) in that control extends not only to who may access which data, but also to how the data may or may not be used or distributed afterwards.

In addition to access control requirements, usage control introduces requirements about the further usage of data once it has been given to somebody else, so-called *obligations*. Examples include "data must not be further distributed" and "data must be deleted within 30 days". As introduced in [3], we classify obligations according to their *controllability* and *observability*. Dedicated mechanisms may be used for controlling and observing the fulfillment of obligations, and thus help with the enforcement of usage control requirements. Such mechanisms can for example be found in the area of digital rights management (DRM) [2].

2 Assignment

2.1 Objectives

The goal of this project is to create a taxonomy of mechanisms that can be used for controlling the fulfillment of obligations. The projected outcome of the project is a survey of different existing mechanisms, and a categorization of those according to suitable criteria.

3 Tasks and Deliverables

The following tasks are part of the project.

- Getting familiar with current work on concepts, policies and architectures in the area of usage control [1, 3].
- Creating a working definition of "control mechanism".

- Creating a survey of technical and non-technical mechanisms that fit into the above definition.
- Extracting key criteria for categorizing control mechanisms.
- (optional extension) Defining a syntax and semantics for describing the capabilities of control mechanisms within vocabularies.
- (optional extension) Extending the survey to observation mechanisms. This task is only possible if it is not done within the Master's Thesis "Monitoring Usage Control Requirements".

The main deliverables of the project shall be the survey of control mechanisms, and the categorization of those.

At the end of the project, a presentation of 20 minutes must be given during an Infsec group seminar. It should give an overview as well as the most important details of the work. The final report may be written in English or German. Three copies of the final report must be delivered to the supervisor.

4 Approval

February 16th 2006

Prof. D. Basin

References

[1] M. Hilty, D. Basin, and A. Pretschner. On obligations. In *10th European Symposium on Research in Computer Security (ESORICS)*, pages 98–117, 2005.

[2] Q. Liu, R. Safavi-Naini, and N. P. Sheppard. Digital rights management for content distribution. In *Australasian Information Security Workshop (AISW)*, 2003.

[3] A. Pretschner, M. Hilty, and D. Basin. Usage Control, 2006. To be published in CACM.