Authorization Architectures for Privacy-Respecting Surveillance

Ulrich Flegel and Michael Meier

University of Dortmund, D-44221 Dortmund, Germany
{ulrich.flegel|michael.meier}@udo.edu

Abstract. Even more than in our physical world, in our digital world we need systems that meet the security objective of service providers and users in equal measure. This paper investigates the requirements of secure authorizations with respect to accountability and privacy in the context of surveillance for misuse detection during service utilization. We develop a model of system architectures for secure and privacy-respecting authorizations that allows to derive and compare the properties of available technology. It is shown how the model maps to existing authorization architectures.

Keywords: Architecture, authorization, privacy, pseudonym, surveillance, misuse detection, intrusion detection.

1 From Physical to Digital: A Short Visit to the Zoo

Many safeguards in the digital world mimic safeguards in the physical world. The reason probably is that safeguards are necessary, if the actors do not trust each other. However, at the end of the day, trust is usually anchored in the physical world. Using an example it is shown how we deal with trust in the physical world. In the following, we describe the case of a student who wants to visit the zoo. In the example the zoo serves as a service provider offering free admission to students. Non-students might feel tempted to defraud the zoo by pretending to be a student in order to obtain free admission. Hence, the personnel at the zoo ticket booth is instructed not to trust statements that customers make about their own property as a *student*. For customers it is thus insufficient claiming to be a *student*, also because the ticket booth personnel cannot verify the statement without considering supporting documents. Instead, it is required to show a valid student ID. The student ID is used as a certified property statement that assigns the name of the subject of the statement to the property *student*. At the ticket booth a certified property statement is accepted, if it is a student ID, as a matter of policy the issuing university is trusted to generate useful property statements, the person on the picture visually matches the presenting person, the student ID has not yet expired and looks "genuine".

If the student ID is accepted at the ticket booth, the presenting person is authorized to pass the zoo entrance. The presenting person receives the service-specific property *authorized for zoo entrance*. Therefore customers that are *authorized for zoo entrance* receive an admission ticket at the ticket booth. The

J. Lopez, P. Samarati, and J.L. Ferrer (Eds.): EuroPKI 2007, LNCS 4582, pp. 1–17, 2007.

ticket is accepted at the zoo entrance, if the stated ticket booth is trusted to issue tickets only to persons that are *authorized for zoo entrance*, the ticket number looks "plausible", the ticket authorizes to pass the zoo entrance, it has not yet expired and looks "genuine".

If the admission ticket is accepted at the zoo entrance, the student may enter the zoo. Right in the front is a sign that specifies behavior that is by policy prohibited in the zoo. Most notably, it is prohibited to tease the monkeys, since they may take revenge using banana peel projectiles. Thus, for the time being, the zoo trusts that the visitors stick to the rules. At critical areas (at the monkey house) the zoo may put a guard in place. The guard observes the behavior of the visitors and reacts, if he detects a violation of the zoo policy.

This paper presents a model for authorization architectures and criteria for deriving and comparing generic high-level properties of existing privacy-enhancing technologies when applied to surveillance for misuse detection. The model and criteria are developed in four steps:

- Generalizing the hybrid PKI model of Biskup and Karabulut [1] by abstracting from PKI-specific technology an architecture model for secure authorizations is developed, which primarily meets the security interests of service providers (see Sect. 2).
- Our previous work on pseudonyms [2] is generalized for the model to solve the privacy problems created by surveillance data, thereby enabling lawful misuse detection. What distinguishes our pseudonym approach from related work is the integrated notion of technical purpose binding for pseudonym disclosure (see Sect. 3).
- Combining the model from Sect. 2 with pseudonyms results in an architecture model for secure and privacy-respecting authorizations (see Sect. 4).
- Given the model, criteria are developed to derive and compare generic high-level properties of privacy-respecting authorization architectures (see Sect. 5). It is shown how the model can be applied to existing privacy-enhancing technologies (see Sect. 6).

The proposed model is compared to existing models in Sect. 7 and the paper concludes in Sect. 8 with a summary of the contributions.

2 An Architecture Model for Authorizations

Based on the assumption that services do not generally trust in property statements that users make on their own behalf, authorization architectures rather rely on property statements that are responsibly certified by agents trusted by the service. In the proposed model individuals, computers and other players in a distributed IT system are denoted as *entities*. A *principal* is a bit string that is unique within its scope of application and it is associated with an entity to serve as its surrogate. An entity can enjoy *properties*, which in turn may be used in conditions in authorization policies, and are taken into account during the trust evaluation.