

Authorizations

Section 2.1 motivates to examine trust and safeguards for authorizations by using examples from the real, i.e. physical, world in order to develop an analogous model for authorizations in the digital world, starting with an example of real-world authorizations in Sect. 2.2. Necessary conditions for trust and control are considered in Sect. 2.3. The constructions used in Sect. 2.2 are mapped to constructions in the digital world in Sect. 2.4 and elaborated as a model for secure authorizations in Chap. 3.

2.1 From the Real World to the Digital World

Many safeguards in the digital world mimic safeguards in the real/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 finally anchored in the real world.

In the following, we consider trust and safeguards in the real world to understand the models presented in this Part. The models in turn help us to classify and distinguish available privacy-enhancing technologies in the digital world and to infer their properties. While the exposition in the first seven Chapters of this Part has a wide scope, the models are developed to focus on audit data pseudonymization.

2.2 Visiting the Zoo – Example Real-world Authorizations

Using an example it is shown how we deal with trust in the real 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*. The name of the university is stated as the agent that is responsible for the correct assignment. An embedded picture indicates that the subject name actually is the name of the person visually matching the person on the picture. Finally, the property statement comprises information regarding its validity, e.g. expiry, and features of genuineness that are expensive to counterfeit. 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*. At the zoo entrance, again, it is insufficient claiming to be *authorized for zoo entrance*. The lack of trust, again, is reasonable, since anyone could defraud the zoo by cheating in order to pass the entrance for free. Therefore customers that are *authorized for zoo entrance* receive an admission ticket at the ticket booth. This authorization comprises a ticket number, the statement that it *authorizes for zoo entrance*, identifies the issuing ticket booth, validity information, such as features of genuineness that are expensive to counterfeit¹ and expiry. The 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”. Note, that the ticket contains no information to authenticate the presenting person, i.e. it is transferable. Further possibilities for cheating are hinted at by the apostrophes (“...”).

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. It is highly unlikely that anyone will responsibly certify that the student will avoid all prohibited behavior, i.e. that the student has the property *policy-compliant-behavior*. Thus, for the time being, the zoo trusts that the visitors stick to the rules. At critical areas (at the monkey

¹ That is, the cost of counterfeiting the validity information is higher than the admission price.

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.

2.3 Trust and Control

Section 2.2 describes two situations where service-specific *givers* (here: zoo ticket booth, zoo entrance) give something. The process of giving is subject to conditions over properties as defined by the policy of the giver (here: *student, authorized for zoo entrance*). If the *taker* can put the *giver* at a disadvantage by cheating w.r.t. the properties required by the *giver*, the *giver* cannot rely on the respective property statements of the *taker*. Instead, the *giver* wishes to verify by himself the required properties of the *taker*. Only then he knows that the *taker* enjoys the required property, and the *giver* himself can assign the property to the *taker*. In case the *giver* cannot carry out the verification by himself, he needs to trust a third party (here: university, zoo ticket booth) to carry out the verification, to assign the property statement to the *taker* and to provide it with features of genuineness that are expensive to counterfeit (here: student ID, admission ticket), i.e. to responsibly certify the property statement. Using appropriate property statements the third party trusted by the *giver* may delegate the verification and certification to other parties that it trusts. Delegation and licensing are not within the scope of this text, however, they integrate seamlessly with the models we present [18, 19, 125].

Since the *taker* may be interested in corrupting the process of certification, he must not be able to control the trusted third party. Specifically, only the trusted third party must be able to provide the property statements that it certifies with features of genuineness. If these requirements are satisfied, the *giver* can trust that the required property in a certified property statement exists and is correctly assigned to the *taker*.

In some environments or applications it is impossible or not intended to employ property verification preventively, e.g. to enforce compliance of behavior with a certain policy. In these environments or applications, taking will be prohibited or sanctioned if the property *policy-compliant-behavior* is violated. That is, for the time being, the *giver* needs to trust that the *taker* enjoys the required property and he may observe (here: guard) the *taker's* behavior at critical areas (here: monkey house) to detect violations of the policy.

2.4 Real-World Counterparts in the Digital World

In the digital world the preventive property verification using certified property statements corresponds to access control, e.g. using a public key infrastructure

(PKI). Also in the digital world it is not always useful or possible to preventively verify all properties, such as policy compliance of behavior of the users or processes of an IT system. However, the IT system can record the observable behavior in the form of audit data, which can be analyzed w.r.t. policy violations, e.g. using intrusion detection systems (IDS) [147, 3, 6].



<http://www.springer.com/978-0-387-68254-9>

Privacy-Respecting Intrusion Detection

Flegel, U.

2007, XX, 307 p. 61 illus.,

ISBN: 978-0-387-68254-9