Project Description:

Surveillance Camera

Application Scenario

Currently, surveillance cameras are being used more and more widely. This raises important questions of privacy: In most democratic countries, it is considered unacceptable to mass record surveillance data without a warrant or even a suspicion.

Thus, the company RoboEye Inc. wants to build a system that can mitigate at least some of these privacy concerns. The idea is to record data and then store it in such a way that it can not be retrieved without a warrant. Since different countries and usage scenarios have very different access rules, the system is to support any possible access structure. As an example, if in a certain situation, it requires the town judge, the town sheriff, and one out of three bank directors to access the recordings, then the system is to make exactly this type of access possible.

You are hired as a consultant by RoboEye Inc. Your task is to design a solution that protects data on the way from the camera to the database, and in the database itself. You have to make sure that your solution allows only legitimate users to access the respective parts of the database and that it supports a variety of different access structures. Note that different entries in the database can have different access structures!

Hint: It is recommended to look up the basics of *secret sharing* for this project.

Project Definition

Design, evaluate, and document a surveillance camera solution that addresses the issues presented by the scenario outlined above. Issues that *must* be addressed are:

- Risk analysis: What assets are at stake?
- Threat model: What assumptions do you make about the attacker(s), and what threats is your system supposed to protect against? In particular, remember that several parties could co-operate in order to get illegitimate access to the data.
- Security: Make sure that your system protects against the security issues raised in the threat model, and clearly document the threats that you do not protect against.
- Key Management: Remember that whenever a key owner looses his access rights (i.e., due to job change or retirement), the system has to be adapted in an appropriate way.