Project Description:

Public Transport

Application Scenario

In many countries current paper-based ticketing solutions for pubic transport systems have been or are currently being replaced by electronic solutions. Many of these first-generation systems have security problems: cloning of cards is technically not too difficult, and the privacy of the users is not protected in any way.

In this despite the commonly accepted view that concerns about privacy are among the most frequent reasons for people not buying goods and services online or not using electronic alternatives to paper based systems that do offer some privacy.

You are hired as a consultant by a national public transport operator. Your task is to design a solution that prevents operators from assigning detailed usage profiles to user identities while at the same time allows for convenient billing and attractive fares.

Hint: It is recommended to look up the basics of *pseudonyms* for this project. It is also recommended to consider and critically evaluate commercial solutions that are currently available, like e.g. the NXP Mifare product line.

Project Definition

Design, evaluate, and document a public transport billing 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?
- 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.