

Security Model Checkers for Smart Card Protocol Design

Motivation

Formally specifying interactive protocols has the advantage that the correctness of the protocol state machine can be verified by automated means. In the recent years various activities took place within the security community to include security aspects in the formal protocol design. Using formal methods in the design of security protocols is very important because it is very hard to find by hand attack paths in complex state machines.

Project description

- Goals
 - State of the art survey
 - Feasibility study
- Tasks
 - Understand Theory
 - Security & Crypto (protocols and primitives)
 - Logics
 - Knowledge Engineering
 - Write a survey
 - Study feasibility of different techniques
 - study applicability to smart cards
 - study trade off between level of abstraction and security
 - the study phase shall be done on a given informal/semi-formal description of protocols.

Literature

- www.avantssar.eu

Deliverables

- Survey (state of the art)
- Feasibility study
- Presentation (10 .ppt slides)

Project schedule

- Start Immediately
- Month 1 State of the art survey
- Month 2 Start feasibility study
- Month 3 Continue feasibility study

Master Project

Studies: INF SEW TEL Tech. Math.

Prerequisites

- interest in Theory

Advisor / contact

Roderick.Bloem@iaik.tugraz.at

wolfgang.steinbauer@nxp.com

Joint Project with NXP