Model-based Testing of Electronic Passports

Wojciech Mostowski, Erik Poll, Julien Schmaltz,
Jan Tretmans, Ronny Wichers Schreur

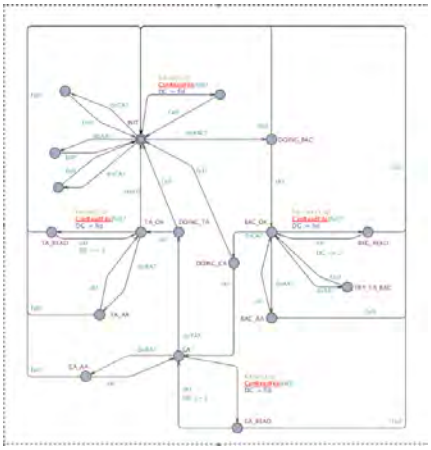
Electronic Passports

Electronic passports contain a contactless smartcard with a picture and personal data of the holder. New European passports will also contain fingerprints. Several security mechanisms are in place to safeguard the authenticity and confidentiallity of this data. We were involved in a project to test the security in a real-world implementation of the electronic passport.

The Specs

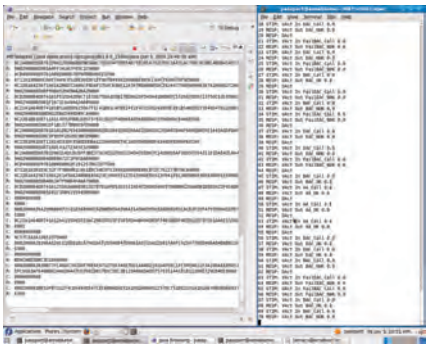
The basic protocols are specified in an ICAO standard. This standard references many other standards. Implementators of the standard have various options in their choice of protocols. Also, the standard is underspecified, in particular for error conditions.

The Model



After scrutinising the specifications we constructed a formal model of the passport's behaviour. This model takes the form of a labelled-transition system. The model contains explicit transitions for error conditions.

The Tools



The model was fed to the testing tool TorXakis (based on TorX) that automatically generates and executes test cases on the fly. The JMRTD framework provided the Java implementations of the protocols. Also jUnit was employed for *ad-hoc* testing.

Experiences

Understanding the specifications and constructing the model was most of the work. After that using TorXakis to automatically run test cases was quick and easy. We started with a coarse model, which allowed us to run tests early on in the project. The model was then subsequently refined. In this project model-based testing has clearly proven its value.

Radboud Universiteit Nijmegen
LaQuSo Laboratory for Quality Software
Embedded Systems Institute