Smart cards protocols

Ondřej Klubal
xkluba00@stud.fit.vutbr.cz

The topic of my PhD thesis is called Invasive Methods of Attacks on Chips. It is in fact focused to various attack methods including even non-invasive ones and semi-invasive. Invasive attacks are most powerful, but require most expensive equipment for chip depackaging and provide unlimited possibilities of chip function modifying. Semi-invasive also needs chip to be depackaged, but change of internal chip state is for example caused by x-rays, light or electromagnetic fields. Non-invasive methods needs only access to external chip interface and uses side channel attacks or communication protocol vulnerabilities to reveal chip secrets.

Smart cards and Radio-frequency identification (RFID) chips are widely used for storing cryptography secrets. Most of these cards can be found in security-sensitive applications like financial services (e.g. Credit cards), telecommunications (e.g. SIM cards), governmental services (e.g. biometrics passwords), and pay TV systems.

This essay will focus at chip cards protocols and their formal analytics. Tools for automatic protocol testing are based on SAT model checking or tree automata, which are known from theoretical computer science. At first we will take a look on languages for describing cryptographic protocols. Then we will focus on specific case, using tree automata. This includes steps from informal and formal semantics to the abstract model.