Electronic passport and biometrics, winter 2006

MICHAEL NÜSKEN

6. Exercise sheet
Hand in solutions until Tuesday, 12 December, $12^{\underline{15}}$.

Exercise 6.1 (Basic Access Control). (5 points)

(i) On the usage of the chip's first random number `RND.ICC`: What happens if you try to communicate with the chip and playback a communication with the chip? (Note that an attacker might first record a communication and then steal the passport chip and then try to get more information by inducing errors in the chip using strong magnetic or electric fields for example while repeating the recorded communication.) 1

(ii) Reanalyze: which information do we need to get the information in the chip? In particular, is it enough to steal the passport (and place it back later)? 1

(iii) Does a read operation leave any trace on the passport? Should it? 1

(iv) Are hash collisions a danger? Describe an "attack" that uses a hash collision to forge a passport (or two) with a wrong picture. And explain how to prevent it. 1

(v) If someone gets hold of the document signer's private key she can forge a passport. Of course, as soon as this gets noticed the key will be revoked. How could an attacker still successfully cross the border with the forged passport? 1

Exercise 6.2 (Generation of pseudo random numbers). (3+1 points)

We consider the electronic passport.

(i) Where are pseudo random numbers used? 1

(ii) Does it help an attacker if she can predict the produced pseudo random numbers? 1

(iii) How are they generated? +1

(iv) Which requirement is set for this generation? (Compare 5.1.2.2 in the common criteria protection profile.) 1