Esecurity: secure internet & e-passports, summer 2011

MICHAEL NÜSKEN, RAOUL BLANKERTZ

13. Exercise sheet
Hand in solutions until Sunday, 10 July 2011, 23:59

Exercise 13.1 (Challenge Semantics). (9 points)

(i) What prevents chip cloning? How does it work? $\boxed{2}$

(ii) Describe the differences between Chip Authentication and Active Authentication. $\boxed{2}$

(iii) Instead of sending a (meaningless) nonce as challenge in the Active Authentication protocol one could send an (unpredictable) meaningful challenge, containing among other things the date, the time and the location of the terminal. What does the chip's reply proof later on? How could this approach be misused? What kind of threat is introduced by this? $\boxed{4}$

(iv) Is such a challenge semantic attack possible with chip Authentication? $\boxed{1}$

Exercise 13.2 (Advanced Security Mechanisms). (10 points)

(i) Is a man-in-the-middle attack against PACE possible? Explain. $\boxed{2}$

(ii) What is the purpose of the Terminal Authentication Protocol? Under which assumptions can Version 2 be considered secure? Describe the security model. Can an attacker with the power to factor quickly break the scheme, if RSA is used in the protocol? $\boxed{4}$

(iii) Why is Terminal Authentication before Passive Authentication in the General Authentication Procedure? $\boxed{2}$

(iv) The BSI suggests to combine Chip Authentication and Passive Authentication. Consider a man-in-the-middle attack on this combination. $\boxed{2}$

Exercise 13.3 (Restricted Identification). (0+6 points)

As disused in the lecture, Passive Authentication and Chip Authentication provide unique identifiers. But with without this authentication the terminal can not trust the chip.

+6 How does Restricted Identification work?

Exercise 13.4 (What to ask.). (4+6 points)

4+6 Think about what you have learned during the semester. Formulate and answer at least one appropriate exam exercise.