Esecurity: secure internet & e-passports, summer 2014

MICHAEL NÜSKEN

11. Exercise sheet
Hand in solutions until Monday, 30 June 2014, 13:00

Exercise 11.1 (Myths about e-Passports!?). (10 points)

(i) Read MIKE ELLIS (2010). 39 Myths about e-Passports: Part I-III. *ICAO MRTD Report* **5**(1-3). URL `http://tinyurl.com/owvtzpj`. See also `http://www.gemalto.com/govt/inspired/myths_about_epassports/myths.html`. [0]

(ii) Judge Myth # 11. [2]

(iii) Verify the numbers in Myth # 33 and present them in bits. Are they reasonable? Compare with your results from Exercise 10.2. Why is — according to the author — the low entropy of the MRZ no threat? [2]

(iv) Choose your two favorite myths (except # 11 and # 33) and find for each myth a source in which the myth is claimed to be true. Give a short summary of the source and why it is claimed to be only a myth. Judge the statements made by either sides. [6]

Exercise 11.2 (Challenge Semantics). (9 points)

(i) What prevents chip cloning? How does it work? [2]

(ii) Describe the differences between Chip Authentication and Active Authentication. [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? [4]

(iv) Is such a challenge semantic attack possible with chip Authentication? [1]

Exercise 11.3 (Advanced Security Mechanisms). (8 points)

2 (i) Is a man-in-the-middle attack against PACE possible? Explain.

4 (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?

2 (iii) Why is Terminal Authentication before Passive Authentication in the General Authentication Procedure?