Esecurity: secure internet & e-passports, summer 2011

MICHAEL NÜSKEN, RAOUL BLANKERTZ

12. Exercise sheet
Hand in solutions until Sunday, 03 July 2011, 23:59

Exercise 12.1 (Traceability). (7 points)

(i) Read TOM CHOTHIA & VITALIY SMIRNOV (2010). A traceability attack against e-passports. In *14th International Conference on Financial Cryptography and Data Security 2010, LNCS*. Springer. URL `http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.169.1985`. [0]

(ii) Passports from which countries were tested? [1]

(iii) What is the special flaw in the French e-Passport in this context? [2]

(iv) Describe the "time-based traceability attack" in general. [4]

Exercise 12.2 (Myths about e-Passports!?). (10 points)

(i) Read MIKE ELLIS (2010). 39 Myths about e-Passports. *In ICAO MRTD Report Vol. 5 No. 1-3.* URL `http://www2.icao.int/en/MRTD/Downloads/Forms/AllItems.aspx`. [0]

(ii) With Exercise 12.1 in mind judge Myth # 11. [2]

(iii) Verify the numbers in Myth # 33 and present them in bits. Are they reasonable? Compare with your results form exercise 11.2. 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 12.3 (primary biometric identifier). (4 points)

In the lecture you discussed "Why ICAO selected the face as primary biometric identifier specified to epassports". Consider the voice of a person as biometric identifier and comment whether the arguments for the ICAO's decision still hold or not. 4