Esecurity: secure internet & e-passports, summer 2014

MICHAEL NÜSKEN

7. Exercise sheet
Hand in solutions until Monday, 26 May 2014, 13:00

Exercise 7.1 (Authentication in IKEv2). (8 points)

(i) Read RFC 5996 again (do not forget Section 2.15, 3.6, and 3.8) and explain how the authentication in IKEv2 works.

(ii) What are the possible schemes for authentication mentioned in the RFC? Are there more in the up to date IANA assignments? [2]

(iii) What kind of certificates are designated? [2]

(iv) Choose one of these authentication schemes and describe the authentication process for your choice in detail (step-by-step). What are the pros and cons for your choice? [4]

Exercise 7.2 (Project, part 2). (5+5 points)

Consider your chosen protocol (TLS/SSL or SSH) for this exercise.

(i) Discuss the security of the chosen protocol under the same security aspects as we did for IPsec: [5+5]

(a) Session key agreement.

(b) Perfect forward security.

(c) Denial of Service.

(d) Endpoint identifier hiding.

(e) Live partner reassurance.

We will summarize your results in the course and tutorial soon.