Esecurity: secure internet & e-passports, summer 2011

MICHAEL NÜSKEN, RAOUL BLANKERTZ

6. Exercise sheet
Hand in solutions until Sunday, 15 May 2011, 23:59

Exercise 6.1 (IKEv2 parameter). (4 points)

(i) Read RFC 5996.

(ii) Which block cipher algorithms can be used in IPsec/IKEv2? [1]

(iii) Describe the groups for the Diffie-Hellman key exchange that can be used in IKEv2. [3]

Exercise 6.2 (IPsec and IKEv1 criticism). (8 points)

(i) At `http://www.schneier.com/paper-ipsec.html` you find the IPsec and IKEv1 criticism of Niels Ferguson and Bruce Schneier. Read and summarize it. (What are their recommendations? What are their major reasons? Do they say whether IPsec/IKE is secure or how to make it secure?) [4]

(ii) Reconsider their arguments in the presence of IKE version 2 (that we discussed in the course). [4]

Exercise 6.3 (SSL and SSH). (6 points)

Choose whether you consider TLS/SSL or SSH for this exercise.

(i) Where is your chosen protocol located in the OSI-model? What are pros and cons of this placement? [2]

(ii) How is the start of a communication specified and how is the key exchange done in your chosen protocol? [4]