Esecurity: secure internet & evoting, summer 2010

MICHAEL NÜSKEN, KONSTANTIN ZIEGLER

4. Exercise sheet
Hand in solutions until Sunday, 16 May 2010, 23.59 h

Exercise 4.1 (IPsec in practice). (4 points)

Which (common) applications do use/implement IPsec? 4

Where is it used in our vicinity? (Where within b-it, computer science Bonn, computer science Aachen, University Bonn, University Aachen? Which services there do use it?)

Exercise 4.2. (8 points)

(i) At `http://www.schneier.com/paper-ipsec.html` you find the IPsec and IKE v1 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 4.3. (4 points)

IPsec is working between the network and the transport layer of the OSI-model. Contrary to this, SSL is situated between the transport and the session layer. What are pros and cons of each placement? 4