Security on the Internet, summer 2006

MICHAEL NÜSKEN

7. Exercise sheet

Hand in solutions on Tuesday, 4th of July, at the b-it info desk. Deadline for any completely signed(!) electronic solution is the same Tuesday, 23:59.

Exercise 7.1 (IPsec in practice). (0+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 of Bonn, University of Aachen? Which services there do use it?)

Exercise 7.2 (Authentication and Encryption). (4 points)

When you want to sent a signed and encrypted message, in which order should the operations be applied? Make a statement and argue. 4

Compare to IPsec/ESP with both options.

Exercise 7.3 (1999 IPsec criticism). (4 points)

At `http://www.schneier.com/paper-ipsec.html` you find the IPsec and IKE criticism by Bruce Schneier and Niels Fergusons. 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

Exercise 7.4 (IKE). (4 points)

(i) Show how someone who knows both Alice' and Bob's public encryption key (and neither side's private key) can construct an entire IKE exchange based on public encryption keys that appears to be between Alice and Bob. 2

(ii) Design a protocol in which one side has a public signature key and the other side has a public encryption key. 2