9. Exercise sheet
Hand in solutions until Monday, 20 June 2016, 11:59

Exercise 9.1 (Project, part 1). (16+12 points)

Choose either OTR/Axolotl or EMV for this exercise. Make your choice public via http://doodle.com/poll/xg52m2a6qk25ntv6.

Find sources that describe the chosen protocol and study them. These sources should include the relevant up-to-date RFCs if any.

(i) Supply a list of all used sources! 2
(ii) Give a short description of the protocol (in your own words!), enough to answer the following questions. 2
(iii) Where is the chosen protocol (typically) located in the OSI-model? What are pros and cons of this placement? 2
(iv) How is the start of a communication specified and how is the key exchange done in the chosen protocol? Is a man-in-the-middle attack possible? Does the key exchange include cipher negotiation, if so how? 6
(v) How is the data transfer secured? Which authenticated encryption schemes are allowed? 4
(vi) Discuss! +12

Exercise 9.2 (Authenticated encryption). (8 points)

(i) Read Rogaway & Wagner (2003). 1
(ii) What is authenticated encryption? 1
(iii) Briefly describe the CCM mode. 3
(iv) Summarize the criticism made in the paper. 4

References