# Esecurity: secure internet & e-cash, summer 2012

Michael Nüsken, Raoul Blankertz

## 7. Exercise sheet
## Hand in solutions until Sunday, 3 June 2012, 23:59

**Exercise 7.1** (Project). (18+12 points)

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

Find sources that describe the chosen protocol and study them. These sources should include the relevant up-to-date RFCs. Supply a list of all used sources! Give a short description of the protocol (in your own words!), enough to answer the following questions.

(i) Where is the chosen protocol located in the OSI-model? What are pros and cons of this placement? $\boxed{2}$

(ii) 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? $\boxed{4}$

(iii) Discuss the security of the chosen protocol under the same security aspects as we did for IPsec: $\boxed{12+12}$

(a) Session key agreement.

(b) Perfect forward security.

(c) Denial of Service.

(d) Endpoint identifier hiding.

(e) Live partner reassurance.

(f) Plausible deniability.

(g) Stream Protection.

(h) Negotiating parameters.

We will summarize your results in the course and tutorial on 5 June.

**Exercise 7.2** (CBC-MAC). (9 points)

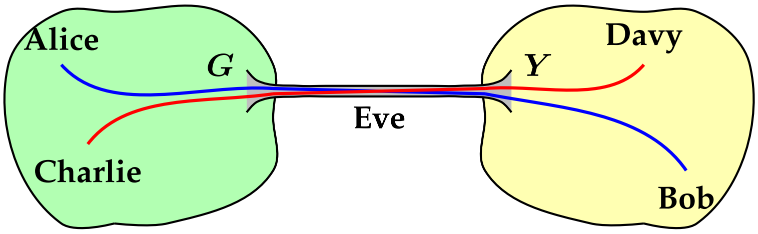
Consider a block cipher in CBC mode and a CBC-MAC with the same underlying block cipher.

$\boxed{3}$ (i) What happens if we use for both schemes the same key? Which blocks can be changed while keeping the MAC tag valid?

$\boxed{3}$ (ii) Assume we choose the initial vector for the MAC randomly and send it along with the message and the MAC tag. How can an attacker change the message?

$\boxed{3}$ (iii) Given two pairs of message and MAC tag $(m, t)$ and $(m^*, t^*)$, can an attacker somehow concatenate them to achieve a longer message with valid MAC tag?

**Exercise 7.3** (Splicing Attack). (8 points)



Suppose that the gateways $G$ and $Y$ link the green and the yellow LAN by an encrypted but not authenticated IPsec tunnel using a fixed SA. Assume that the encryption is done by some symmetric cipher in CBC mode. We want to show that Eve and her boss Davy can read all the traffic between Alice and Bob.

$\boxed{2}$ (i) How does the beginning of a packet from Charlie to Davy look like?

$\boxed{2}$ (ii) Replace the beginning of a packet from Alice to Bob or from Bob to Alice with the start of an eavesdropped packet from Charlie to Davy. What happens?

$\boxed{2}$ (iii) How can Davy find out the part just after the replaced beginning? [Consider retransmitting. . . ]

$\boxed{2}$ (iv) Draw conclusions. [Formulate a proposal, explain, argue.]

(v) Go beyond.