Esecurity: secure internet & e-voting, summer 2013

MICHAEL NÜSKEN

9. Exercise sheet
Hand in solutions until Monday, 17 June 2013, 08:00

Exercise 9.1 (CBC-MAC). (9 points)

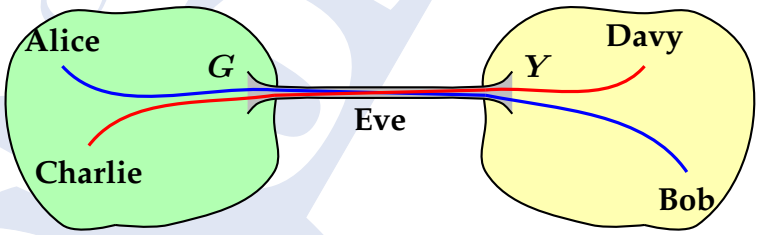
Consider a block cipher in CBC mode and a CBC-MAC with the same underlying block cipher.

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

Exercise 9.2 (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.

(i) How does the beginning of a packet from Charlie to Davy look like? 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? [2]

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

(iv) Draw conclusions. [Formulate a proposal, explain, argue.] [2]

(v) Go beyond.