The art of cryptography, summer 2016

MICHAEL NÜSKEN

8. Exercise sheet
Hand in solutions until Monday, 13 June 2016, 11:59

Exercise 8.1 (TLS documentation). (8+4 points)

Find the basic, up-to-date RFC for TLS and 'read' it.

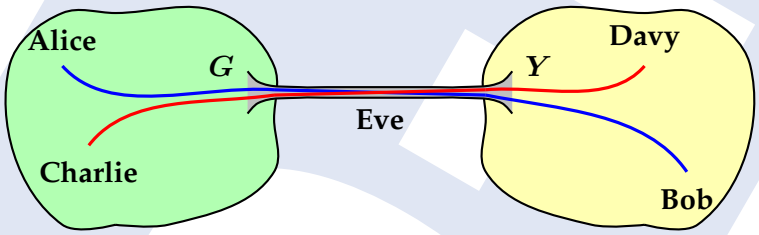
(i) How is the Client's Finished message composed if the client does not have a certificate? [3]

(ii) Under which conditions is forward security provided? Can the client force it? Can the server force it? [3]

(iii) Does the protocol provide live partner reassurance? (Otherwise an attacker can *replay* possibly modified old messages.) [2]

(iv) Break the newest version of TLS. [+4]

Exercise 8.2 (Splicing Attack or: unauthenticated!). (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.