Esecurity: secure internet & e-passports, summer 2014

MICHAEL NÜSKEN

6. Exercise sheet
Hand in solutions until Monday, 19 May 2014, 13:00

Exercise 6.1 (Project, part 1). (8+12 points)

Choose either TLS/SSL or ssh/scp for this exercise. Make your choice public via `https://doodle.com/vfqquidbcbn7vqgp`.

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!

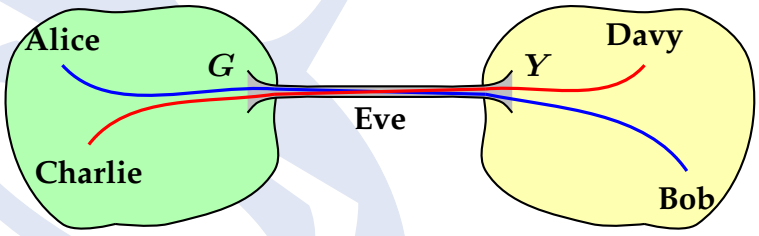
(i) Give a short description of the protocol (in your own words!), enough to answer the following questions. [2]

(ii) Where is the chosen protocol located in the OSI-model? What are pros and cons of this placement? [2]

(iii) 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? [4]

(iv) Discuss! [+12]

Exercise 6.2 (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.

Exercise 6.3 (IKEv2 parameters). (10 points)

(i) Read RFC 5996.

(ii) If a Security Association (SA) expires, how can a new (valid) SA be negotiated? [2]

(iii) After rekeying, may the new SA have cryptographic schemes being different from the old one? [1]

(iv) What is a "Nonce"? How is it used in IKEv2? How long must a nonce be? May it be chosen deterministically? [3]

(v) Which block cipher algorithms can be used in IPsec/IKEv2? Give an up to date list. [1]

(vi) Describe the groups for the Diffie-Hellman key exchange that can be used in IKEv2. In particular, are elliptic curves among them? [3]