Esecurity: secure internet & e-passports, summer 2014

MICHAEL NÜSKEN

9. Exercise sheet
Hand in solutions until Monday, 16 June 2014, 13:00

Exercise 9.1 (Capturing IPsec, SSH and SSL). (0+12 points)

For the this exercise we recommend to use the tool "´Wireshark"´. For privacy reasons, do not include the whole captured pcap files in your assignment (unless you have anonymized them)!

(i) Capture an IPsec connection from your computer to the b-it (`https://www-sgbit.bit.uni-bonn.de/wiki/doku.php?id=pnas_en:vpn`).

(ii) Capture an SSH connection from your computer to `login.bit.uni-bonn.de`.

(iii) Capture an SSL connection from your computer to `https://en.wikipedia.org/wiki/Main_Page`.

(iv) Answer the following questions for each captured connection.

(a) Which version of the respective protocol was used? Is it the up to date version? +3

(b) Which cryptographic schemes were proposed and which were chosen? +3

(c) Are there identifiers which identify the client? The server? +3

(d) Describe the key exchange. How many messages where exchanged before the key exchange started? Which key exchange scheme was used? How is it authenticated? +3