The art of cryptography, summer 2017

MICHAEL NÜSKEN

6. Exercise sheet
Hand in solutions until Friday, 23 June 2017, 11:59

Exercise 6.1 (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 6.2 (Capturing TLS). (8+4 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 a TLS connection from your computer to the b-it (`https://cosec.bit.uni-bonn.de/`). 2

(ii) Answer the following questions for the captured connection.

(a) Which version of the protocol was used? Is it the up to date version? 1

(b) Which cryptographic schemes were proposed and which were chosen? 1

(c) Are there identifiers which identify the client? The server? 1

(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

(iii) Do it again with another target with major differences. (Maybe an IMAP connection?) +4

Exercise 6.3 (DNSSEC KSK Rollover). (0+8 points)

Read `http://www.heise.de/netze/meldung/DNSSEC-Verfahren-fuer-Schluesseltausch-in-der-Rootzone-festgelegt-3208629.html` and summarize. +8
(First hand information can be found at `https://www.icann.org/resources/pages/ksk-rollover`.)

In particular: What is the problem? What is the purpose of DNSSEC and its root-key? Why is it so complicated to exchange it? Which consequences could a manipulation have?