Esecurity: secure internet & e-voting, summer 2013

Michael Nüsken

8. Exercise sheet
Hand in solutions until Monday, 10 June 2013, 08:00

Exercise 8.1 (Vulnerability of TLS). (13+5 points)

(i) Read `http://www.isg.rhul.ac.uk/tls/TLStiming.pdf`.

(ii) Give a short overview of the described attack. $\boxed{2}$

(iii) Which powers/sources does an attacker need? $\boxed{3}$

(iv) Describe each step of the attack along with a judgment of feasibility. $\boxed{4}$

(v) Why is the attack called Lucky Thirteen? $\boxed{1+3}$

(vi) Quickly describe the idea behind the suggested countermeasures. Is the attack still feasible in the latest version of TLS? $\boxed{3}$

(vii) Read up on the so called "‘BEAST"’ attack and summarize (see for instance `https://bugzilla.mozilla.org/show_bug.cgi?id=665814`). $\boxed{+2}$

Exercise 8.2 (Authenticated encryption). (8 points)

(i) Read Rogaway & Wagner (2003).

(ii) What is authenticated encryption? $\boxed{1}$

(iii) Briefly describe the CCM mode. $\boxed{3}$

(iv) Summarize the criticism made in the paper. $\boxed{4}$

Exercise 8.3 (Capturing SSH and SSL). (0+8 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 SSH connection from your computer to `login.bit.uni-bonn.de`.

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

(iii) Answer the following questions for both captured connections.

$\boxed{+2}$ (a) Which version of the respective protocol was used? Is it the up to date version?

$\boxed{+2}$ (b) Which cryptographic schemes were proposed and which were chosen?

$\boxed{+2}$ (c) If there are any identifiers, which identifies the client and which the server?

$\boxed{+2}$ (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?

References

P. ROGAWAY & D. WAGNER (2003). A Critique of CCM. Technical Report 070. URL `http://eprint.iacr.org/2003/070`.