Esecurity: secure internet & e-cash, summer 2012

MICHAEL NÜSKEN, RAOUL BLANKERTZ

8. Exercise sheet
Hand in solutions until Sunday, 10 June 2012, 23:59

Exercise 8.1 (Vulnerability of SSL). (14+2 points)

(i) Read Bard (2004).

(ii) Give a short overview of the described attack. 2

(iii) How does the *weak variant* of CBC differ from the standard one? Guess, why the weak variant is used nevertheless. 2

(iv) Which powers/sources does an attacker need? 3

(v) Describe each step of the attack along with a judgment of feasibility. 4

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

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

Exercise 8.2 (Authenticated encryption). (8 points)

(i) Read Rogaway & Wagner (2003).

(ii) What is authenticated encryption? 1

(iii) Briefly describe the CCM mode. 3

(iv) Summarize the criticism made in the paper. 4

References

GREGORY V. BARD (2004). Vulnerability of SSL to Chosen-Plaintext Attack. URL `http://eprint.iacr.org/2004/111`.

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