Esecurity: secure internet & evoting, summer 2010

MICHAEL NÜSKEN, KONSTANTIN ZIEGLER

6. Exercise sheet
Hand in solutions until Sunday, 06 June 2010, 23.59 h

Exercise 6.1 (*Vulnerability of SSL (I)*). (20 points)

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

(ii) Describe the attack model. 4

(iii) How does the *weak variant* of CBC differ from the standard one? Guess, why the weak variant is used nevertheless. 3

(iv) Which powers/sources does an attacker need? 4

(v) Describe each step of the attack along with a judgment of feasibility. 6

(vi) Quickly describe the idea behind the suggested countermeasures. 2

(vii) Is the attack still feasible in the latest version of TLS? 1

Exercise 6.2 (*Vulnerability of SSL (II)*). (10 points)

(i) Read CHRISTOPHER SOGHOIAN & SID STAMM (2010). Certified Lies: Detecting and Defeating Government Interception Attacks Against SSL. URL `http://ssrn.com/abstract=1591033`.

(ii) Describe the attack model. 4

(iii) Describe the idea behind the CertLock solution. 3

(iv) Why should sites consider the country of the CA they use? 3