Esecurity: secure internet & e-passports, summer 2011

Michael Nüsken, Raoul Blankertz

8. Exercise sheet Hand in solutions until Sunday, 29 May 2011, 23:59

Exercise 8.1 (Vulnerability of SSL (I)). (12+8 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. $\boxed{4}$

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

(iv) Which powers/sources does an attacker need? $\boxed{4}$

(v) Describe each step of the attack along with a judgment of feasibility. $\boxed{+6}$

(vi) Quickly describe the idea behind the suggested countermeasures. $\boxed{+2}$

(vii) Is the attack still feasible in the latest version of TLS? $\boxed{1}$

Exercise 8.2 (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. $\boxed{4}$

(iii) Describe the idea behind the CertLock solution. $\boxed{3}$

(iv) Why should sites consider the country of the CA they use? $\boxed{3}$