Security on the Internet, summer 2006

MICHAEL NÜSKEN

8. Exercise sheet

Hand in solutions on Tuesday, 11th of July, at the b-it info desk. Deadline for any completely signed(!) electronic solution is the same Tuesday, 23:59.

Exercise 8.1 (Denial of Service). (3+3 points)

Read Steve Gibson, "The Strange Tale of the Denial of Service" at `http://www.grc.com/dos/grcdos.htm` (say, at least up to the FBI part).

(i) Suppose your site only accepts IPsec packets. Consider the case that this attack is launched on your site and see whether you are better protected against it. [2]

(ii) Which modifications to IPsec would you suggest to increase its ability to withstand such an attack? [1]

(iii) Ask further questions. (Formulate at least two.) [+1] [+2]

Exercise 8.2 (SSL/TLS). (6 points)

Consider the following questions. Don't forget to 'proof' your answers.

(i) Which common services do use SSL or TLS? [2]

(ii) How does SSL/TLS prevent reflection attacks? [1]

(iii) Does SSL/TLS provide perfect forward security? [1]

(iv) Can Eve find out the endpoints? [1]

(v) Do we have Live Partner Reassurance? [1]