Christian Schindelhauer

Freiburg, 2016-01-22
Joan Bordoy
Sebastian Sester

Exercise No. 12
Peer-To-Peer Networks
Winter 2015

Exercise 1 *TCP Tahoe*

Consider the following transmission:

1. S = 32 KB, ssthresh = 8 · S
2. Packet 8 and 16 get lost

Draw the first 20 transmissions. Assume the use of TCP Tahoe.

Exercise 2 *Basic security terms*

Explain each of the three main goals of security:

1. Confidentiality
2. Integrity
3. Availability

Also, name and explain an attack for each of the three.

Exercise 3 *(Distributed) Denial of Service attacks*

Explain whether DoS- and DDoS-attacks are the same in regard to:

1. The result
2. How easy or difficult the attack can usually be blocked
3. The basic systematics behind the attack

Exercise 4 *AES / RSA*

Explain whether (and why) you would use RSA or AES in the following situations:

1. Encrypted transfer of a large file
2. Secured, but unencrypted transfer of a large file
3. Sending a large mail to a person which is not online at the moment you're writing the mail.