technische universität
dortmund

Fakultät für Informatik
Lehrstuhl 4

M. Sc.-Inf. Dimitri Scheftelowitsch
M. Sc.-Math. Alexander Frank

Winter term 2016/17

Computer Networks and Distributed Systems
Exercise Sheet 14

Publication: January 30, **Discussion:** February 7–10, **submission not mandatory**

Quiz questions

1. Describe the different parties in a typical security scenario.
2. Differentiate between symmetrical and asymmetrical cryptography.
3. Describe the purpose of a digital signature.
4. Differentiate between message integrity and message authenticity. Is it possible to enact integrity without authenticity? Is it possible to enact authenticity without integrity?

Exercise 14.1

We consider various attacks on communication and the resulting requirements for a secure communication protocol.

(a) Describe the *known ciphertext* attack. Which properties should an encryption protocol fulfill to render this attack hard to impossible?

(b) Describe the *man in the middle* attack. How can an authentication protocol be designed to counter this attack?

(c) Describe the *chosen plaintext* attack. How could an encryption protocol be designed to make this kind of attack hard to impossible?

Exercise 14.2

We consider the inner workings of a firewall.

(a) On which layers does a firewall work?

(b) Describe the function of the different filter types in a firewall.

(c) How is it possible to detect a firewall before a host?

Exercise 14.3

(a) SNMP messages are being sent over UDP (instead of TCP). Why?

(b) SNMP knows two types of message modes: request-response and traps. What are the pros and cons of these modes with respect to overhead, reaction time on exceptional events, robustness to message loss?