Technische Universität München
Lehrstuhl Informatik VIII
Prof. Dr.-Ing. Georg Carle
Dr. Heiko Niedermayer
Cornelius Diekmann, M.Sc.
Dr. Ralph Holz

Network Security Winter Term 2014/2015
Exercise 1

Exercise 1 Understanding security goals

a) What are the 5 security goals, as defined in the lecture (technical definition)?

b) Discuss: What is more important, confidentiality or integrity?

c) For each of the 5 security goals, find a scenario where the respective goal is the most important.

Exercise 2 Passwords and computational effort

a) The recommended password length for offline applications (e.g. disk encryption) is significantly higher than that for online applications (e.g. Web-based login): at least 12-14 characters versus at least 8-10 characters (given a Latin alphabet, plus numbers and special characters). What is the crucial difference between the two applications that makes it possible to make do with shorter passwords in the online case?

b) Given the same underlying alphabet and randomly chosen password characters, which password is stronger: (1) a password of 8 characters consisting of upper case and lower case letters, numbers, special characters, etc. or (2) a password of 12 characters consisting only of lower case letters? Give the general formula to determine the password's strength and explain which factor in the formula is the most important one in making a password strong?

Exercise 3 Attackers

a) What are the two types of network-level attackers?

b) What can each attacker do?

c) Suppose you are sending messages over the Internet. Are there some attacks which are never detectable (independent of the security services you are using)? Are there some attacks where it may not be decidable whether it is caused by an attacker or just a random error?

Exercise 4 Symmetric Encryption (Exam 2012)

a) Explain how a block cipher works.