Exam 2: Security in Networks

27.5.2

To pass 5.5 points are needed. Maximum 10 points can be achieved. Thus, you have the flexibility to choose to answer two of the following questions 2, 3, 4 (note, if you solve all three questions, i.e. 2, 3 and 4, then only two of them will be count).

1. Assume that you are only allowed to use the 26 characters from the alphabet to construct passwords. *(1+1+1+1)*
   - How many different passwords are possible if a password is at most n, n = 4,6,8, characters long and there is no distinction between upper case and lower case characters?
   - How many different passwords are possible if a password is at most n, n = 4,6,8, characters long and passwords are case sensitive?
   - Assume that passwords have length six and all alphanumerical characters, upper and lower case, can be used in their construction. How long will a brute force attack take on average if
     - it takes one tenth of a second to check a password?
     - it takes a microsecond to check a password?
   - Are NP-complete problems a suitable basis for constructing security algorithms?
2. Let (L, ≤) be a lattice of security levels where L is a finite set. *(1+1+1)*
   - Show that unique elements System Low and System High must exist in such a lattice.
   - You are given a security policy stating that a subject has access to an object if and only if the security level of the subject dominates the security level of the object. What is the effect of using the lattice with this policy for users, guests and root?
   - Which label should be assigned to the root directory of a multi-level secure operating system?
3. The placement of a security function in a system determines its functionality and practicality. *(1+1+1)*
   - Classify the freedom of placement in a network? Discuss the advantages and disadvantages of the placement.
   - Where would you put the anonymity function? Explain your choice.
   - Can you have security without security kernels? Discuss the advantages and disadvantages of having a security kernel as the TCB.
4. DC-Network and Message Service are the two anonymity techniques providing information theoretic security. *(1+1+1)*
   - Describe shortly the protocols.
   - What are the main similarities and what are the main differences?
   - Sketch the idea of information theoretic security and explain why DC-Network and Message service are capable to provide this strength of security!