S

LiTH, Linköpings tekniska högskola

IDA, Department of Computer and Information Science
Nahid Shahmehri

Written exam
TDDD17 Information Security
2015-06-08
14-18

Permissible aids
English dictionary (printed, NOT electronic)

Teacher on duty
Marcus Bendtsen, 0733-140708

Instructions
There are 5 general questions and 5 in-depth questions. The general questions are from G1 to G5, and the in-depth questions are from D1 to D5. The questions are grouped pair-wise under their corresponding topic.

You may answer at most 3 general questions and 3 in-depth questions. You may answer both the general and the in-depth question for *at most one topic*. If you answer more than 3 general or 3 in-depth questions, we will randomly discard excess answers. If you answer both questions for more than one topic, we will randomly discard answers for all but one of the affected topics.

Students who have completed one or both of the optional labs in 2015 will get bonus points on the exam. Each completed lab gives 2 bonus *in-depth points*. Note that you must still fulfil the minimum requirement for points from general questions to pass the exam (see below).

You may answer in Swedish or English.

Grading
A correct answer for a general question gives you 2 points, and a correct answer for an in-depth question gives you 6 points. To pass the exam you need to accumulate at least 3 points from general questions and 9 points from in-depth questions or lab bonus points. The exam grading depends on the total number of accumulated points.

The following grading scale is preliminary and might be adjusted during grading.

Grade	C (3)	B (4)	A (5)
Points required	12	17	21

System Security

G1 Give a simple real-life (i.e. *not* computer related) example of Role-Based Access Control (RBAC). Make sure to explain what the roles are in your example, and how they relate to the access controls.

D1 In the lectures, three Java security models are discussed. Explain what they are, and give a high-level explanation of how they work.

Identification and authentication, Biometric user authentication

G2 Define uniqueness and permanence related to biometric traits. Indicate why these seldom are true premises in practical systems.

D2 Attacks at the user interface: Discuss how impersonation, obfuscation and spoofing may be exploited to breach the security of a biometric system!

Network security

G3 Briefly explain how behavior-based and knowledge-based NIDS work (maximum 30 words).

D3 Security associations (SA), security policy databases (SPD) and security association database (SAD) are three integral parts of IPsec. Explain what they are, what they contain, and how they work together. Your answer should be detailed, should include examples of entries in the SPD and SAD, and it should be clear how the three combine to make IPsec work.

Risk analysis

G4 Give two different examples of qualitative risks. If you can only mitigate one of them, how can you systematically compare them in order to choose which one to mitigate?

D4 Explain the ISRAM risk analysis method. It should be clear from your explanation what is done in each step, which equations/tables are used, and you should give examples of the output from each step. In order to structure your response, come up with a simple scenario where you can apply ISRAM and then explain the method by applying it to this scenario (it is not necessary that your risk analysis is complete, only that every step is carefully explained and exemplified).

Business continuity planning, Disaster recovery planning, Physical security

G5 In the context of database recovery, explain remote journaling and remote mirroring.

D5

a) Explain how ALE values are calculated. Make sure that you explain each factor, and when possible, break down the factor to its individual components and explain these as well.

b) Describe three scenarios that threaten different physical security aspects and mechanisms that would work towards mitigating these risks.