LiTH, Linköpings tekniska högskola
IDA, Department of Computer and Information Science
Nahid Shahmehri

Written exam
TDDD17 Information Security
2011-03-14
8-12

Permissible aids
Dictionary (printed, NOT electronic)

Teacher on duty
Anna Vapen, 073-849 12 75

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 passed the labs in 2011 can assume their in-depth question for the network security topic (D3) answered.

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. 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 Explain the role of the Java Security Manager in relation to Java security.

D1 Virtualization is increasingly common. Explain what virtualization is, how it relates to security. Discuss the limitations/risks involved in using virtualization technology (with respect to security).

Identification and authentication, Biometric user authentication

G2 Enumerate the seven basic requirements categories, which are listed in the course literature as suitable for evaluation of a biometric system! Include a short explanation of each in at most one sentence! You are not required to remember the exact words, as long as you remember all seven aspects to evaluate.

D2 List at least three different hardware attack methods aiming at finding a stored key in a token! Describe shortly what is done in the attack, and describe shortly at least one countermeasure for each attack type! No points are given for just the name of an attack. They must be correctly described, but the whole answer should not cover more than two A4 sheets. Any additional sheets will not be read. Attacks using only deficiencies in the software access control or in the logic of communication protocols are not regarded as hardware attacks.

Network security

G3 Give an example of how an Internet attack can successfully target a system that is not connected to the Internet.

D3 Explain the CIDF model of intrusion detection systems. Explain the purpose of each component in the model. Explain one limitation network-based intrusion detection systems (NIDS) have compared to host-based intrusion detection systems (HIDS). Give an example of an attack that could be detected by a HIDS, but probably not by a NIDS.

Risk analysis

G4 How is a risk evaluation matrix used to reason about risks?

D4 What does it mean to assess a risk and why is it important for risk management?

Business continuity planning, Physical security

G5 What can an attacker find by searching a site for error and warning messages using Google?

D5 Explain the terms *breadth*, *depth*, and *deterrence*, and the connection they have to each other. In physical security, why is it not enough with only one property out of *breadth*, *depth*, and *deterrence* when planning a defense?