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

Written exam
TDDD17 Information Security
2010-03-09
8-12

Permissible aids
Dictionary (printed, NOT electronic)

Teacher on duty
Anna Vapen, 013-288986

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 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 Name and briefly describe two basic functions in a trusted platform.

D1 Explain the process of trusted boot. What are the security consequences of not having trusted boot?

Identification and authentication, Biometric user authentication

G2 The course literature introduces the terms FMR and FNMR as alternatives to the earlier prevalent FAR and FRR. In the text this is motivated by possible confusions regarding the result of the false decision. You can, however, also argue that we should distinguish between two totally different causes for the risk of a false match/acceptance. What are the two totally different phenomena, which both can cause a false match/acceptance? Which of these two cannot be properly included in a probabilistic rate curve, and why is this so?

D2 In Maltoni et alt. a lot of points are defined on the typical curves showing FMR and FNMR for a biometric system as functions of the allowed measurement variation. Two such points are the ZeroFMR and the ZeroFNMR. ZeroFMR is defined as the lowest FNMR where no false matches occur. ZeroFNMR is defined as the lowest FMR where no false non-matches occur. Draw a figure showing a possible configuration for the curves and mark the ZeroFMR and ZeroFNMR points! What can these points tell you about suitable settings for a system? Will both these points exist for all possible curve pairs? Motivate! If only one of these two points exists, which is more likely to exist in your opinion? Motivate!

Network security

G3 Explain what a security association is in IPSec.

D3 Network firewalls are excellent security devices for perimeter protection, but do not provide a complete security solution.

Describe the three most probable reasons that a firewall can fail to provide security against threats on the Internet. For each of the reasons/situations/threats you list, also explain a mechanism (or set of mechanisms) that could complement the firewall to provide good security.

Risk analysis

G4 What is the difference between risk analysis and risk management?

D4 Explain what a risk analysis is. What factors have to be taken into account and why? In addition, you shall give an example of a risk analysis using a method of your choice (Except What-if/Checklists) and explain how the method works.

Business continuity planning, Physical security

G5 Explain why the following Google query can be considered as useful for the security assessment of web servers? intitle:index.of -pub

D5 Assume that you as the physical security practitioner at the company have secured the outermost perimeter as the first physical layer of defense. Your options for security here were walls and gates with ID checks. Working from the next ring inwards, list the physical layers and also a couple of common options for the security in each physical layer that remain in your careful securing of the company and its facility.