Försättsblad till skriftlig tentamen vid Linköpings Universitet

Datum för tentamen	2012-05-21
Sal	TER1
Tid	14-18
Kurskod	TDDD17
Provkod	TEN1
Kursnamn/benämning	Information Security, Second Course
Institution	IDA
Antal uppgifter som ingår i tentamen	10 (5 general and 5 in-depth)
Antal sidor på tentamen (inkl. försättsbladet)	4
Jour/Kursansvarig	Anna Vapen / Nahid Shahmehri
Telefon under skrivtid	073-8491275
Besöker salen ca kl.	15, 17
Kursadministratör (namn + tfnnr + mailadress)	Madeleine Häger-Dahlqvist (013-282360, madeleine.hager.dahlqvist@liu.se)
Tillåtna hjälpmedel	Dictionary (printed, not electronic)
Övrigt (exempel när resultat kan ses på webben, betygsgränser, visning, övriga salar tentan går i m.m.)	Preliminary grading: C(3): 12 points, B(4): 17 points, A(5): 21 points

LiTH, Linköpings tekniska högskola

IDA, Department of Computer and Information Science
Nahid Shahmehri

Written exam
TDDD17 Information Security
2012-05-21
14-18

Permissible aids
Dictionary (printed, NOT electronic)

Teacher on duty
Anna Vapen, 073-8491275

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 2012 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 what a rootkit is, and why rootkits are so dangerous.

D1 **a)** Which design principle(s) can RBAC be used to implement?

b) Imagine a simplified Webreg system with only one course (security course) with the following functions: create a new year of the course; edit information about the course; create assignment; edit assignment; delete assignment; record assignment result; report final grades; register for course; view own results; view all results.

Assume the existence of the following users:
Ted: responsible for the security course
Ava: lab assistant in the security course
Sarah: student in the security course

Instantiate RBAC for this application. Your answer should detail roles, transactions and authorizations. Explain your answer in detail.

Identification and authentication, Biometric user authentication

G2 Assume that the performance of a biometric system is expressed in terms of False Acceptance Rate (FAR) and False Rejection Rate (FRR). As responsible for the security, your task is to set the threshold η that defines the FAR and FRR of the biometric system. You decide to increase η to decrease FAR and increase FRR, explain how 1) the security level of the biometric system is affected and 2) how the use of the biometric system can affect the persons using it.

D2 Face recognition is one method for biometric recognition. Describe how such a biometric system operates, including an overview of how the face images are used for identification/authentication. Mention at least three factors that affect the performance of the system and explain the consequences.

Network security

G3 How can IPSec be used (i.e. which protocol(s)) to provide data integrity and confidentiality of the contents of a TCP connection.

D3 Which steps are typically involved on an attack on a system that is not directly accessible to an attacker? For each step, name and briefly explain one security mechanism that could be used to prevent, detect or mitigate that step of the attack. If no mechanism is applicable at one or more of the steps, explain why.

Risk analysis

G4 Give a reason why you need a "monitor and review activity" in a risk management process.

D4 Explain how the risk management activity "Establish context" carries through and affects the each and every other activity in a risk management framework. Be clear in explaining what is affected in each activity and in what way it is affected.

Business continuity planning, Physical security

G5 What is physical security, and what does it secure?

D5 Name and explain the 5 stages of a Business Impact Assessment (BIA). Explain the process of preparing a quantitative analysis for your BIA.