Försättsblad till skriftlig tentamen vid Linköpings Universitet

Datum för tentamen	2014-03-17
Sal	T1, T2
Tid	8-12
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	Marcus Bendtsen / Nahid Shahmehri
Telefon under skrivtid	0733-140708
Besöker salen ca kl.	09:00, 11:00
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
2014-03-17
8-12

Permissible aids
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 passed the labs in 2014 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 What is the principal difference between Mandatory Access Control (MAC) and Discretionary Access Control (DAC)?

D1

a) What is a *sandbox*? What secure design principle is the sandbox concept based on? Give an example of a technology mentioned during the lectures that can be used to implement sandboxes.

b) Briefly describe an attack that could be prevented by running a web browser inside a sandbox.

c) What is a *reference monitor* in the context of sandboxes? What secure design principle should one try to adhere to when designing and implementing a reference monitor? Motivate your answer!

Identification and authentication, Biometric user authentication

G2 What are the main (four) building blocks of a biometric system according to the course literature? What are their respective main roles in a biometric system?

D2 Identify and discuss factors of importance when considering a physical or behavioral trait to be used in a biometric application! (Hint: The literature mentions seven such factors. Whether you in the discussion are using precisely these seven terms is not the main point, but that your discussion is valid and sound is important.)

Network security

G3 Intrusion detection systems can be modelled as four boxes. What are the names and functions of these boxes? Explain in general terms what an attack on each of these boxes hopes to achieve.

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 Explain what is meant by risk and what it means to mitigate a risk. Give two different examples of how risks can be mitigated.

D4 Explain the 7 steps of CORAS. It is important that you explain in detail the activities of each step and who are involved in these activities. For each step also explain what documents are produced, and what they are used for.

Business continuity planning, Disaster recovery planning, Physical security

G5 What are the differences between cold, warm, hot and mobile alternate sites?

D5 The company CAB offers a global communication service to medium sized businesses. They have an office in Seattle which is used mainly by sales and marketing, but also for customer meetings. Their servers (running both services and databases) are placed in a facility located in the north of Sweden. Their users (i.e. the employees of their customers), are mainly active in four cities: Tokyo, New Dehli, Melbourne and Los Angeles. You are in charge of BCP, DRP and physical security for CAB.

Your answers to the following should be reasonable and take into consideration that CAB works on a limited budget. Answers should be based upon topics discussed in this course.

BCP - Come up with three assets and three business functions that are important for CAB. For each asset and for each function, think of an event that will affect the asset/function. Add ALE values to the assets given the event, and show how you derived them. Add MDT/RTO values to the functions (again, given the event you came up with). Come up with three qualitative risks that are important for CAB. Create a priority list combining assets, functions and qualitative risks.

DRP - CAB relies heavily on their databases and servers. Come up with two events that could cut off the Seattle office from the databases and two events that could cut off CABs customers from CABs services. Suggest detailed actions that mitigate the risk of these four events effecting CAB and their customers.

Physical security - The office in Seattle hosts both employees (sales and marketing) and customers. Describe five scenarios that threaten different physical security aspects and mechanisms that would work towards mitigating these risks.