Försättsblad till skriftlig tentamen vid Linköpings Universitet

Datum för tentamen	2014-06-09
Sal	TER3
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)	5
Jour/Kursansvarig	Marcus Bendtsen / Nahid Shahmehri
Telefon under skrivtid	0733-140708
Besöker salen ca kl.	15:00, 17:00
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
2014-06-09
14-18

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 Briefly describe the main ways in which *SELinux* improves upon the traditional access control model of Unix operating systems.

D1

a) Describe the security ring architecture used in common operating systems, such as Windows or Linux.

b) Describe the weakness of the traditional security ring architecture that *ARM TrustZone* aims to address. Give an example! Explain, on a high level, how ARM TrustZone works.

Identification and authentication, Biometric user authentication

G2 What are the three basic methods of person recognition? What is the main advantage of using biometric recognition?

D2 Which questions need to be addressed when evaluating a complete biometric system? In what way are these questions of importance to be able to evaluate a biometric system?

Network security

G3 When designing networks for security, what are the three main concerns? Explain each concern briefly.

D3 Network intrusion detection systems generally consist of four boxes. Explain three different attacks that target the E-box. For each one of the attacks explain how the attack is performed, why it theoretically could work, and what the consequences are of a successful attack.

Risk analysis

G4 We can use both qualitative and quantitative measures to reason about risk. Choose either (state clearly which one you choose), and give two examples of quantified risks. Assume that only one can be mitigated; explain how we can compare the two risks in order to choose which one to mitigate.

D4 Consider the following system running at a small business:

One incoming Internet connection from an ISP into a wireless capable router (R1). From the router two workstations (W1 and W2) are directly connected by cable. A server (S1) is also connected by cable directly to the router. Finally a laptop (L1) is connected using wireless. The business runs a web-server on S1, which should be reachable from anyone on the Internet. W1, W2 and L1 should all have Internet access.

Complete a CORAS risk analysis on this system. Pick only a small number of assets and threats to work with, it is not important that the risk analysis is exhaustive, but it must be realistic. The focus of your response should be on the actual steps completed as part of CORAS. Important to note: If you make any assumptions then state them clearly. Your response should explain exactly what is done in each step of CORAS, and you should draw examples of necessary diagrams, charts, figures and tables. It is very important that you are clear what is going on in each step.

Business continuity planning, Disaster recovery planning, Physical security

G5 What are the four steps of business continuity planning? Give a summary of what is done in each step.

D5 You are the chief information security officer (CISO) at a medium-sized company known as CAB. As part of your duties you are responsible for BCP, DRP and physical security. The company has never evaluated their BCP, DRP and physical security before, and so it is your task to do so now. Make your own assumptions about what CAB does and answer the following. (Your answers should be reasonable and clear. 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 - Come up with two events that could severely affect CAB's possibility to perform their core operations (the consequence of the events should not be the same). Suggest detailed actions that could mitigate the risk of these two events.

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