Försättsblad till skriftlig tentamen vid Linköpings Universitet

Datum för tentamen	2014-08-22
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)	4
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
2014-08-22
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 Give an example of how virtualization can improve the security of a computer system.

D1 Explain how disk encryption using BitLocker with a Trusted Platform Module (TPM) differs from a software-only solution, where the user simply supplies a password to decrypt the file system. What is the main security benefit? Motivate your answer with an example.

Identification and authentication, Biometric user authentication

G2 Define identification and (identity) verification! What is the main difference regarding complexity and computations between the two?

D2 Insider attacks: Discuss how collusion, coercion, negligence, enrollment fraud and exception abuse may be exploited to breach the security of a biometric system!

Network security

G3 You are in charge of setting up a new network for your company, and you have decided to only use wires (i.e. no wireless). Are risks associated with wireless networking completely mitigated? If not, then give an example of a risk that is not mitigated.

D3 Explain in detail and give examples of four different challenges that face any implementation of network intrusion detection systems (NIDS).

Risk analysis

G4 Give two different examples of quantitative risks and quantify them. If you can only mitigate one of them, which one should you choose, and why?

D4 A company in need of a website is considering installing a web server at their office to host the site. Before deciding to do so, they would like to know about the potential risks and the necessary precautions to mitigate these risks.

Complete a CORAS risk analysis over this decision. 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 clearly state what is going on in each step.

Business continuity planning, Disaster recovery planning, Physical security

G5 Explain four different ways of conducting training and testing of a disaster recovery plan.

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. CAB has an office building in Seattle (A1) and a downtown retail store in Los Angeles (A2). It is critical that the office can call the retail store (F1) and that the retail store is fully stocked at all times (F2). CAB sells physical security devices, and so it is extra important that there are no break-ins, since it would be bad PR (Q1). Furthermore, employees specialized in security are hard to find, so the work force must be kept happy (Q2).

BCP - Given the assets (A1, A2), the functions (F1, F2) and the qualitative assets (Q1, Q2) you should create a priority list (step 2 in business continuity planning). In order to do so you will need to come up with events that could affect the assets/functions and use several quantitative measures (e.g. MTD) in order to prioritize them. Only come up with one event per asset and one event per function. It is important that you show exactly how you come up with the measures and how they are calculated.

Physical security - Suggest one mechanism that could mitigate the risk of break-ins at the office and another that could mitigate break-ins at the retail store (explain why they would mitigate the risk).