Försättsblad till skriftlig tentamen vid Linköpings Universitet

Datum för tentamen	2013-08-23
Sal	TER2
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	David Byers / Nahid Shahmehri
Telefon under skrivtid	013-282821
Besöker salen ca kl.	15:30
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
2013-08-23
14-18

Permissible aids
Dictionary (printed, NOT electronic)

Teacher on duty
David Byers, 013-282821

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 2013 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 meant by a time-of-check-to-time-of-use (TOCTTOU) attack (or vulnerability)?

D1 Name and briefly explain the three basic functions in a TCG trusted platform.

Identification and authentication, Biometric user authentication

G2 In a particular biometric system finger prints are used as the biometric identifier. Liveness detection is also used in the system. Explain what liveness detection is and what it is used for! Briefly explain one attack against the system! The attack should be successful even with the liveness detection.

D2 At LiU, RFID cards are used for access control when passing through doors after office hours. Assume that the cards were to be replaced with a biometric system. Which biometric identifier do you think would be the most suitable? Motivate your choice! Explain how the biometric system would work and what pros and cons it has compared to using cards. Explain at least one attack against the biometric system.

Network security

G3 If an attacker can perform DNS cache poisoning against an ISP, what are the potential consequences?

D3 How is network traffic processed using IPSec (both incoming and outgoing). You must explain how the sending system determines if and how to process a given network packet, what is then done with the packets, and how the receiving system processes the traffic it receives.

Explain and illustrate using a concrete example. You use the following example or invent your own of similar complexity:

All e-mail traffic (TCP destination port 25) from system A (IP address 1.1.1.1) to system B (IP address 2.2.2.2), and the corresponding return traffic (i.e. TCP source port 25 from 2.2.2.2 to 1.1.1.1), must be encrypted using ESP with AES and key ID 0x1EE7, with data integrity enabled.

Risk analysis

G4 Explain why risk prioritization is important in the risk management process.

D4 Explain each step of the CORAS risk analysis method and illustrate the diagrams used in the different steps. In addition, explain whether the method is a quantitative or qualitative analysis method.

Business continuity planning, Physical security

G5 Explain how physical security is related to information security!

D5 A medium sized logistics company with several different departments has decided to start using business continuity planning (BCP). The BCP team consists of the following people:

Alice: Head of the IT-department.
Bob: Newly employed programmer in the same department as Alice.
Claire: System administrator with security knowledge and some experience of BCP. Claire works on the internal infrastructure department which keeps the servers and networks up and running, cooperating on a daily basis with the IT-department.

a) If you were to add members to the BCP team to improve the team, what skills would these people have, and what roles would they have in the company? You are free to make any assumptions about the company and its employees as long as you motivate your choices and clearly state all assumptions you make!

b) Alice thinks that the fact that the whole BCP team consist only of IT-people is entirely positive and beneficial for the company and the BCP. Do you agree with her? Explain and motivate why or why not!

c) What is the first and most important task for the team to start working on when they begin working with BCP? Motivate!