Försättsblad till skriftlig tentamen vid Linköpings Universitet

Datum för tentamen	2012-08-17
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)	5
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
2012-08-17
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 the security design principle "fail-safe defaults". Give a concrete example of where the principle is applied.

D1 Assume that the Biba model is used to ensure **data integrity**. The following integrity levels are defined: high, medium and low, so that high > medium > low. Assume the following subjects and objects:

Subject	Integrity level
CEO	High
Project leader	Medium
Copywriter	Low
Object	**Security level**
Cooperation agreement	High
Project description	Medium
Press message	Low

Assume that the objects are related to a common project between two companies. The cooperation agreement is a legal document which has high integrity requirements. The project description must be trustworthy, but drafts of press messages do not have any specific integrity requirements.

The CEO can make decisions related to the cooperation agreement; the project leader has the right to change the project description and the copywriter writes press messages (which need to be approved by the project leader or the CEO before being published).

a) Given the Biba model, create the access control matrix for this system. The rights are read (r) and write (w). Clearly write down all assumptions you make.

b) Are there any limitations in which of the objects a subject may read, which you find unsuitable? Explain these limitations and give suggestions of how to solve these problems while still preserving as much as possible of the integrity given by the Biba model.

c) Is there another formal integrity model which would be better suited for the organization than the Biba model? Name the model and explain its main properties.

Identification and authentication, Biometric user authentication

G2 What is the difference between identification and authentication? Give two examples of requirements on authentication.

D2 Explain and compare two different biometrics in detail. What are their main advantages and disadvantages?

Additionally, give the following **for each** of the two biometrics:

a) An example of an application where it is suitable to use (e.g. to grant access to buildings or in airport security checks)?
b) An example of where it is NOT suitable to use and explain why!
c) A detailed explanation of an attack.

Network security

G3 When segmenting a network for security purposes, give one guideline for when to place systems on the same segment, and when to place them on different segments.

D3 Network Address and Port Translation (NAPT, PAT, Masquerading) enables the use of private addresses on systems connected to the Internet. If a LAN is placed behind NAPT, connections cannot be initiated from the Internet to systems on the LAN, and this prevents a number of different attacks and is frequently used as a security mechanism.

Why does NAPT not provide much security in practice? Name and explain at least two different kinds of realistic and common network-related threats that NAPT does not protect against. Name and explain security mechanisms that could be used to mitigate these threats.

Risk analysis

G4 Shortly explain what risk assessment is.

D4 Given the three attribute classes for risk analysis methods below:

1. Quantitative *or* Qualitative
2. Inductive *or* Deductive
3. Single failure *or* Multiple failures (where "multiple failures" means multiple failures in combination is the cause of a failure event)

Explain for **each one** of the three listed classes, which one of the two alternatives (e.g. quantitative or qualitative) that best fits the CORAS analysis method and why the other alternative is not the best fit. **Writing only the answer for each category without any motivation will not give any points.**

Business continuity planning, Physical security

G5 Physical security planning often requires the deployment of the so called Technical Controls. What is the main goal of Technical Controls? Give two examples of mechanisms that implement them.

D5 The Business Impact Plan (BIA) is a step of the Business Continuity Planning (BCP) process. The BIA has a 5-stage methodology. In the first stage of the BIA, priorities are identified, assets are listed and valued, and a maximum tolerated downtime is attributed to each business function. The second stage is dedicated for risk identification. How are the 3 last stages of BIA called? Explain them in detail and show how and which results from one stage are used by the following stages.