Försättsblad till skriftlig tentamen vid Linköpings Universitet

Datum för tentamen	2011-06-07
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	Christian Vestlund / Nahid Shahmehri
Telefon under skrivtid	076-2275570
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
2011-06-07
14-18

Permissible aids
Dictionary (printed, NOT electronic)

Teacher on duty
Christian Vestlund, 076-2275570

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 2011 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 difference between pure and impure virtualization.

D1 **a)** Explain the security design principle "complete mediation".

b) Explain the security design principle "fail-safe defaults", and give a real-world example of an application of this principle.

c) When using SELinux, it is possible to limit the files a program can access to just the ones it needs in order to operate. This is an implementation of an important security design principle. Which one? Explain the principle in detail, and provide a second real-world example of this principle.

Identification and authentication, Biometric user authentication

G2 Suppose that you have evaluated and installed a biometric system for door locks in the company, where you work. The FAR and FRR of the system were very good, 0,01% and 0.05% respectively. But after a time you get a lot of complaints from employees, who can't access their work place in the three attempts, which are allowed before the identity is blocked for an hour. Another employee complains that somebody is obviously using his identity to get a disallowed shortcut through the buildings. And still there are only 50 employees in the company, so it is not a "large numbers" effect. Please explain these phenomena! The explanation is not that the FAR or FRR as given by the supplier are incorrect.

D2 Biometric systems should be evaluated as a whole, not just regarding the actual biometric property used. Consider the different steps in the authentication process as presented in the course slides. Describe an attack aimed at three different parts of the system, and also describe a defense against these attacks! Note that your attacks may depend on the actual biometric property used, but if you find that all of them do, you are probably describing attacks at the same point, not at three different points.

Network security

G3 Briefly explain what a trust relationship is (with respect to network security), and why trust relationships are so important in network security.

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 During a system development lifecycle, when is risk management carried out?

D4 Enumerate and explain the main activities of a risk management process. Make sure that you explain how each activity affects and relates to the other activities.

Business continuity planning, Physical security

G5 Draw a figure and shortly explain what zoning is with regard to layered defense.

D5 Explain each of the seven steps for business continuity planning (BCP). Also explain what the maximum tolerable downtime is and in what step in BCP it is defined.