Försättsblad till skriftlig tentamen vid Linköpings Universitet

Datum för tentamen	2013-03-11
Sal	U14, U15
Tid	8-12
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	0708-282821
Besöker salen ca kl.	9:30, 11
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
2013-03-11
8-12

Permissible aids
Dictionary (printed, NOT electronic)

Teacher on duty
David Byers, 0708-282821

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 Explain the difference between pure and impure virtualization.

D1 Account lockout is a common mechanism for preventing password guessing is to disable an account after three consecutive authentication failures, or lock it out for a period of time (from several minutes to several hours). However, due to a serious drawback in this type of mechanism, it is being phased out in many systems.

a) Which (if any) secure design principle(s) does the account lockout mechanism implement? Which (if any) secure design principles does this mechanism violate? Motivate your answer.

b) In an on-line environment (e.g. a webmail server), the account lockout mechanism has a very serious drawback that an attacker can exploit, that may even outweigh the benefits of the mechanism. What is this drawback?

c) How can the mechanism be altered to avoid the drawback you discuss in (b)? How does that affect the overall effectiveness of the mechanism?

Identification and authentication, Biometric user authentication

G2 Some non-invasive attacks on smart cards use time and power as variables to reveal stored cryptographic keys. Describe in a few sentences, for each of these two variants, how these attacks are in principle carried out.

D2 The course literature (Jain et al) discusses detection of spoofed fingerprints, and gives five methods of detection. List five methods of spoof detection, and briefly discuss advantages and drawbacks of each individual method (maximum two sentences each). Also, the book mentions a common criticism of spoof detection algorithms employed in many commercial biometric systems. Describe the problem and its security implications. What does the book (or you) suggest as a solution to this problem?

Network security

G3 Explain two important limitations when it comes to the security offered by a firewall.

D3 There are several different kinds of firewalls. Explain what characterizes the following kinds of firewalls, and briefly discuss the pros and cons of each type:

a) Packet filter
b) Stateful firewall
c) Application layer firewall

Risk analysis

G4 Give two reasons why risk management always is an iterative (cyclical) process.

D4 Explain the difference between risk analysis and risk management. In addition, describe the activities that separate the two and why each additional activity is necessary to perform in a risk management process.

Business continuity planning, Physical security

G5 Physical security controls are deployed in the following order: deterrence, denial, detection and delay. Explain why the physical security controls are deployed in this order.

D5 The Business Impact Plan (BIA) is the 2nd step of the Business Continuity Planning (BCP) process. The BIA is 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. The next stage is the likelihood assessment. How are the results of the likelihood assessment expressed and what are the sources of information used to determine them? How is the likelihood assessment used in BIA's following stage, the Impact Assessment?