Försättsblad till skriftlig tentamen vid Linköpings Universitet

(fylls i av ansvarig)

Datum för tentamen	2009-08-17
Sal	TER1
Tid	14-18
Kurskod	TDDD17
Provkod	TEN 1
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	Shanai Ardi/Nahid Shahmehri
Telefon under skrivtid	013-282608
Besöker salen ca kl.	15, Otherwise available through telephone
Kursadministratör (namn + tfnnr + mailadress)	Madeleine Häger-Dahlqvist (013-282360, madha@ida.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.)	
Vilken typ av papper ska användas, rutigt eller linjerat	
Antal exemplar i påsen	

LiTH, Linköpings tekniska högskola
IDA, Institutionen för datavetenskap
Nahid Shahmehri

Written exam

TDDD17 Information Security

2009-08-17

14-18

Permissible aids

Dictionary (printed, NOT electronic)

Teacher on duty

Shanai Ardi, 013-282608

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 have to answer at most 3 general questions and 3 in-depth questions. You must answer at least one of the questions for each topic. 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.

Attention

If you answer more than 3 (general) + 3 (in-depth) questions we will randomly choose 3 + 3 answers for correcting the exam, while the rest of the answers will be discarded.

System Security

G1 Explain what mandatory access control is. Explain what discretionary access control is.

D1 If a system used the same labels for integrity levels and confidentiality levels (assuming the Biba integrity model and Bell LaPadula confidentiality model), what would the practical consequences be?

Identification and Authentication

G2 The course literature distinguishes between multimodal systems and multiple method systems. This terminology is not absolute and generally acknowledged, but the division is real no matter what you call them. So what is the difference between a multimodal and a multiple method system? Biometric passports with fingerprints can be regarded as a multimodal as well as a multiple method system. Explain!

D2 The course literature on token security treats many different attacks and defences against these attacks. Suppose that you are involved in the development of a token intended for use as an authenticating device.

List at least three different design principles/precautions, which should be incorporated in the development, and explain why they are necessary!

Network Security

G3 There is a principle in security known as "multi-layer security", which means that an asset is protected by several layers of (ideally differing) security mechanisms. The purpose is to slow an attacker down and to prevent flaws in a single security mechanism from exposing the asset.

Explain briefly how the principle of multi-layer security can be realized when protecting an asset connected to a computer network.

D3 Some firewalls have a feature called "connection tracking". When this is activated, the firewall stores information about the state of every network connection through the firewall, which allows fine-grained control over traffic filtering.

a) Having connection tracking enabled creates a vulnerability not present when connection tracking is off. Explain what that vulnerability is, how connection tracking causes it, and how it can be exploited.

b) A similar vulnerability exists in certain network protocols. Name at least one such protocol and briefly explain how the vulnerability is manifested in that protocol.

c) There is a design principle involved here, applicable to many network protocols. Explain, in principle, how network protocols should be designed to avoid this vulnerability.

Risk Analysis

G4 What are the steps that must be followed in CORAS risk analysis method?

D4 What kind of information does "site" operator in Google queries reveal? Through an example show that how it can be used by hackers?

Business Continuity Planning, Physical Security

G5 Briefly describe two types of testing that can be performed on a BCP.

D5 Describe the input, output and the tasks done in the BIA phase in the context of the BCP planning process.