Försättsblad till skriftlig tentamen vid Linköpings universitet

Datum för tentamen	2017-06-05
Sal (2)	G35(3) G37(16)
Tid	14-18
Kurskod	TDDD17
Provkod	TEN2
Kursnamn/benämning **Provnamn/benämning**	Informationssäkerhet, fk En skriftlig tentamen
Institution	IDA
Antal uppgifter som ingår i tentamen	4
Jour/Kursansvarig Ange vem som besöker salen	Marcus Bendtsen
Telefon under skrivtiden	0733-140708
Besöker salen ca klockan	15:00, 17:00
Kursadministratör/kontaktperson (namn + tfnr + mailaddress)	Madeleine Häger-Dahlqvist, 013-282360, madeleine.hager.dahlqvist@liu.se
Tillåtna hjälpmedel	Dictionary (printed, not electronic)
Övrigt	Preliminary grading: C(3): 20 points, B(4): 26 points, A(5): 30 points
Antal exemplar i påsen	

LiTH, Linköpings tekniska högskola

IDA, Department of Computer and Information Science
Nahid Shahmehri

Written exam
TDDD17 Information Security
2017-06-05
14-18

Permissible aids
English dictionary (printed, NOT electronic)

Teacher on duty
Marcus Bendtsen, 0733-140708

Instructions
There are 4 main questions on the exam. Your grade will depend on the total points you score. The maximum number of points is 34.

Answers in English only

Grading
The following grading scale is preliminary and might be adjusted during grading.

Grade	C (3)	B (4)	A (5)
Points required	20	26	30

1. System Security (10 points)

a) Bus snooping is a physical attack where the attacker reads out sensitive information by eavesdropping on data flowing on buses. Consider ARM TrustZone and Intel SGX. Can either (or both) of these technologies protect from bus snooping? For full score you must provide sufficient technical descriptions of how both systems work to clearly motivate your answer. Answers without any motivation will give no points. (Side note: Some systems are implemented as Systems on Chip where all components of the computer are integrated into the same chip, thereby making bus snooping physically difficult. For this question, assume that attackers have physical access to buses.) (2 points)

b) Explain how a TPM can be used together with hard drive encryption, so that the hard drive can only be decrypted if the system software has not been tampered with. Your explanation should include all the important hardware and software components involved, and relevant technical features of the TPM. (4 points)

c) Pick **two** of Saltzer and Schroeder's secure design principles, and for each of the two, name and describe the principle and give a practical example of where it is applied. (4 points)

2. Identification and authentication, Biometric user authentication (8 points)

a) One way of achieving authentication is via something that you know, such as passwords or PINs. Which are the two other primary ways of achieving authentication? State at least one example for each way! (2 points)

b) In a biometric system when collecting biometric data, several design parameters are of importance. Describe the role and importance of appropriate sensors when collecting biometric data! (2 points)

c) Describe in general terms what constitutes attacks on the interconnections of a biometric system! Exemplify by indicating what man-in-the-middle and replay attacks are! (4 points)

3. **Network security (10 points)**

a) Describe what ”air-gaps” are and how they are useful for network security. Are they good/practical to have and how can they be breached? (2 points)

b) Describe the main principles used in cellular network security (2G/3G/4G). What changed from generation to generation? What are common attacks attempted in cellular systems? (4 points)

c) Suppose you are running an Intrusion Detection System over IPv4 traffic. What kind of packet fields (e.g. destination IP address) can you use for traffic analysis (i.e., those that are not encrypted) if the flow is using: (4 points)

   i. TLS 1.2

   ii. IPsec transport mode ESP

   iii. IPsec tunnel mode AH

4. Risk analysis, cognitive bias, BCP/DRP and PS (6 points)

a) The BCP process consists of four steps. Name these steps, and give a brief description of the activities that are performed within each step. For each step you should capture the most important parts by using a maximum of 60 words. (2 points)

b) In ISRAM a risk quantification table is defined, while in CORAS a risk evaluation matrix is defined. At first glance they may look similar, however they are used quite differently. Explain how they are used in the two respective methods, and explain how the outcomes of using them are different. Remember, that if you introduce a concept, e.g. “consequence value”, then you need to explain what it means and where it comes from. (4 points)