Försättsblad till skriftlig tentamen vid Linköpings universitet

Datum för tentamen	2017-08-18
Sal (1)	TER2(12)
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, Ulf Kargén
Telefon under skrivtiden	0733-140708, 0706-850940
Besöker salen ca klockan	15:00 (Marcus) , 17:00 (Ulf)
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
2017-08-18
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) Give a simple real-life (i.e. not computer related) example of Role-Based Access Control (RBAC). Make sure to explain what the roles are in your example, and how they relate to the access controls. (2 points)

b) Contrast the traditional security ring architecture with that of ARM TrustZone. Give an example scenario where TrustZone would provide a security benefit over the security ring architecture. (3 points)

c) Explain the concept of *sealing* in the context of TCG and TPMs. Give a brief example of a practical application of sealing. (3 points)

d) Today, two-factor authentication is becoming increasingly common. For example, to log on to a certain web site, you may need to provide both a password and a temporary code sent to your mobile phone. Which of Saltzer and Schroeder's secure design principles does two-factor authentication adhere to? Name and briefly explain the principle, and motivate how it relates to two-factor authentication. *Note: Answering with more than one design principle will yield 0 points!* (2 points)

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

a) Define identification vs identity verification. (2 points)

b) What makes universality an important quality when choosing a biometric trait? (2 points)

c) Identify and describe four advantages of multibiometrics. (4 points)

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

a) Draw a picture that shows classification of different types of IDS (2 points)

b) Draw a picture illustrating a corporate network designed according to main security principles. The network should include a public web server, SCADA devices, office workstations, backup and DNS servers, guest WiFi. (4 points)

c) CIA. (4 points)

   i. Which IPsec modes do provide confidentiality for user data?

   ii. How is authentication achieved in TLS?

   iii. Is confidentiality sufficient to provide integrity and why?

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

a) Explain how ALE values are calculated. Make sure that you explain each factor, and when possible, break down the factor to its individual components and explain these as well. (2 points)

b) Explain and compare the two concepts: electronic vaulting and remote mirroring. (2 points)

c) Name and explain four different ways of conducting training and testing of a disaster recovery plan. (2 points)