LiTH, Linköpings tekniska högskola
IDA, Department of Computer and Information Science
Nahid Shahmehri

Written exam
TDDD17 Information Security
2010-08-20
14-18

Permissible aids
Dictionary (printed, NOT electronic)

Teacher on duty
Anna Vapen, 073-849 12 75

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.

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 terms "mandatory access control" and "discretionary access control".

D1 Name and explain three different design principles for security. For each one, indicate a system or network security mechanism that can be used to implement that principle.

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 (no more than seven sentences each!) how these attacks are in principle carried out. (There are several variants, but for full points you should describe one attack using time and one using power.)

D2 The course literature contains a table grading a lot of biometrics as High, Medium or Low for each of the seven characteristics that should be considered when choosing a biometric method. This grading is both old and subjective, but the effort as such is valuable and illuminating when carried out! So grade keystroke dynamics as High, Medium or Low for all seven characteristics and motivate your grading clearly. A grading without a proper motivation is regarded as no knowledge about the graded characteristic.

Network security

G3 In 802.11 wireless networks, management frames are not encrypted or authenticated. Explain one attack that is possible due to this design.

D3 Explain what DNS cache poisoning is, and what consequences a successful DNS cache poisoning attack could have. What design flaw in DNS is exploited to perform a cache poisoning attack against modern DNS implementations? How is it exploited? Name at least one other protocol with a similar design flaw, and briefly explain the security impact of the design in that protocol. Explain one way in which the DNS protocol could be changed (not necessarily in a backwards-compatible way) that would effectively eliminate cache poisoning attacks.

Risk analysis

G4 How is the term "Risk" defined? Shortly explain each part of the definition.

D4 Explain whether the CORAS method is a risk analysis or a risk management method. In addition, give an example using the CORAS method where you explicitly explain each step of the method.

Business continuity planning, Physical security

G5 Explain what a Hot Site and a Cold Site is, respectively, in the context of BCP and disaster recovery and when and why they are used.

D5 Assume that you have been selected as the BCP project leader, responsible for developing a strong BCP for your company. Explain what members should your BCP team consist of as a minimum, according to the CISSP?