LiTH, Linköpings tekniska högskola

IDA, Department of Computer and Information Science
Nahid Shahmehri

Written exam
TDDD17 Information Security
2012-03-05
8-12

Permissible aids
Dictionary (printed, NOT electronic)

Teacher on duty
Anna Vapen, 073-8491275

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 2012 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 What is the purpose of a reference monitor? How does it contribute to security?

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 Give two examples on how to hack a smartcard in terms of usual targets and gained effect.

D2 Assume you are the head of the security department at national government. You are in charge of providing a biometric system for secure access to the national government buildings. Explain what factors you need to consider, and how these factors can be measured. Suggest a technical approach and motivate your choice of biometric system.

Network security

G3 State one reason why a packet-filtering firewall only provides limited protection for end-user client systems (e.g. a Windows workstation).

D3 DNS cache poisoning is a potentially very serious attack. Explain what the consequences of a successful DNS cache poisoning attack could be. Cache poisoning is possible due to a flaw in the DNS protocol. Explain what this flaw is, and propose a way to prevent DNS cache poisoning (at least in practice, in situations where the attacker is unable to examine the DNS query). State what would be required for your solution to be deployed in practice.

Risk analysis

G4 What does it mean to a) reduce a risk and b) accept a risk?

D4 Explain the difference between risk assessment 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 What is the difference between BCP and DRP?

D5 In which functional order should physical security controls be deployed? Detail your answer by explaining the reasons behind such ordering. What is CPTED and in which category (of the ordering above) can CPTED be classified?