LiTH, Linköpings tekniska högskola

IDA, Department of Computer and Information Science
Nahid Shahmehri

Written exam
TDDD17 Information Security
2013-06-03
14-18

Permissible aids
Dictionary (printed, NOT electronic)

Teacher on duty
David Byers, 0708-282821

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 2013 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 fundamental basis for security in ActiveX? Briefly explain the limitations ActiveX security that stem from this approach.

D1 What is meant by a time-of-check-to-time-of-use (TOCTTOU) attack (or vulnerability)? Give a concrete example of such an attack. Give an example of a security mechanism (in the operating system) that could be used to prevent that particular attack.

Identification and authentication, Biometric user authentication

G2 Briefly explain the difference between authentication and identification!

D2 E-passports (also known as biometric passports or digital passports) are becoming increasingly common. Answer the following questions and *motivate your answers!*

a) Explain what an e-passport is and how it differs from passports in general!

b) Describe in detail at least four weaknesses in e-passports!

c) How can the security related to e-passports be improved? Give at least two examples and motivate them well!

Network security

G3 When using WEP (or no security), it is easy to perform denial-of-service attacks against a wireless network. Is the same true in WPA and 802.11i (WPA2)? Explain why or why not!

D3 Rainbow tables are pre-computed tables for password guessing. Such tables exist for e.g. hashed passwords (without salt) and WPA-PSK authentication. Explain at least three different ways to configure or manage a wireless network with WPA that would defeat password guessing using rainbow tables. Briefly explain why your method works, and briefly discuss the pros and cons of each method.

Risk analysis

G4 What does it mean to define a scope of analysis and why is it important to define before starting a risk analysis?

D4 You are the new Chief Information Security Officer for the medical research company InseCure AB, tasked with securing their network. The main parts of their network is a web server, where patients can view and edit their personal data, and a database containing personal as well as medical data. Employees can add and edit medical data to the database both from their office network and remote.

Your task is to perform a security risk analysis for the system described above using the CORAS method. Explain each step of the method. Write down any assumptions you make about the system and during the analysis.

You do not have to identify all possible risks, it is enough with two or three.

Business continuity planning, Physical security

G5 Explain, in a few sentences, what business continuity planning is and what it is used for.

D5 You are responsible for the physical security of the server room at a small company. Explain the following terms in the context of physical security: *deterrence*, *denial*, *detection* and *delay*. For each of the terms, give an example on how you implement it to secure the server room. Which of the four terms do you think is the most important one and why? *Motivate your choice!*