LiTH, Linköpings tekniska högskola

IDA, Department of Computer and Information Science
Nahid Shahmehri

Written exam
TDDD17 Information Security
2011-08-19
14-18

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 2011 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 Explain briefly how a typical boot process works when using a trusted platform model (TPM).

D1 Assume you have a system with three subjects: A, B, and C and objects O1, O2, O3, and O4. Further assume that your system handles the rights "*read*" (r) and "*write*" (w).

Subject A should be able to read and write everything. Subject B should be able to read objects O1 and O2. Subject C should be able to read and write objects O3 and O4.

a) Define access control lists (ACL) that would enforce these access rules. For each ACL, indicate what it is attached to and what it contains.

b) Define capabilities that would enforce these access rules. For each capability, indicate what it is attached to and what it contains.

c) Define and assign security levels, categories, etc. so that as many of the access rules as possible could be enforced by an implementation of the Bell LaPadula model. Which access rules cannot be enforced by Bell LaPadula? Why?

Identification and authentication, Biometric user authentication

G2 FAR and FRR for face recognition have different implications for identification systems, as they are typically used, and for user authentication systems. The difference is in the expected attitude of the user. Which of the two, FRR or FAR (FNMR or FMR) is mostly influenced by this difference, why is this the most influenced one, and what does that mean for suitable values for FAR and FRR in an identification system compared to in a user authentication system?

D2 Choose three of the seven requirement categories for biometric systems! Find for each of these three a biometric property, which must get low ratings for one of the requirements and high ratings for the other two! Thus you should have three biometric properties, one with ratings (Low, High, High) one with ratings (High, Low, High) and one with ratings (High, High, Low) for your chosen categories taken in a fixed order. Motivate your ratings clearly!

Network security

G3 Name the two most important IPSec protocols and state what security services each can provide.

D3 Typical internet attacks follow a fairly predictable pattern. List and briefly explain the steps typically involved in an indirect attack - where the target system is not directly accessible. For each step, name and briefly explain one security mechanism that could be used to prevent, detect or mitigate the step. If no mechanism is applicable at one or more of the steps, explain why.

Risk analysis

G4 What does it mean to mitigate a risk?

D4 Given the four attribute classes for risk analysis methods below:

1. Quantitative *or* Qualitative
2. Inductive *or* Deductive
3. Process specific *or* not process specific.
4. Single failure *or* Multiple failures (where "multiple failures" means multiple failures in combination is the cause of a failure event)

Explain **for each one** of the four listed classes, which one of the two alternatives (e.g. quantitative *or* qualitative) that best fits the CORAS analysis method and why the other alternative is not the best fit. **Only writing down the answer for each category without any motivation will not give any points.**

Business continuity planning, Physical security

G5 Regarding business continuity planning, give two concrete examples of crisis triggers. That is, two events that can activate a BCP program.

D5 Explain the two concepts of layered defense and zoning. In addition, illustrate and explain the difference between zoning and layered defense.