LiTH, Linköpings tekniska högskola
IDA, Institutionen för datavetenskap
Nahid Shahmehri

Written exam
TDDC03 Information Security
2006-03-11

Permissible aids
Dictionary - Book, NOT Electronic.

Teacher on duty
Claudiu Duma, 0739073213.

Instructions and points

There are 6 general questions and 6 in-depth questions. The general questions are G1 to G6, and the in-depth questions are D1 to D6. The questions are grouped pair-wise under their corresponding topic.

You have to answer at most 3 general questions and 3 in-depth questions. You should choose only one question from each topic, so that it will be 3 (general) + 3 (in-depth). 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 answers can be written in English or Swedish.

Attention

If you answer both questions for a certain topic we will randomly discard one of the two answers.

If you answer more than 3 (general) + 3 (in-depth) questions we will randomly choose 3 + 3 answers for correcting the exam, while the rest of the answers will be discarded.

Running code securely

G1 What is meant by code signing? Explain and provide two examples. How much security can you achieve with code signing?

D1 Comment the following statements. Are they true, false or "it depends"? Why? Elaborate your answer.

a) A network worm is an example of the mobile code paradigm of "code on demand".

b) The Java sandbox always denies Java code access to the file system.

c) Partial result authentication codes (PRAC) reliably protect the confidentiality of agent data.

d) keytool is used to verify signed Java code.

e) The Java Security Manager and the Java Access Controller have essentially the same functionality.

f) Both Java and .NET virtual machines support bytecode verification prior to code execution.

Writing secure code

G2 First, explain the difference between functional and non-functional requirements in general. Second, relate functional and non-functional requirements to the security principle "Security features are not (necessarily) secure features".

D2 You are about to construct a login module in a software system. The requirements specification says "The system shall be constructed in C/C++", "The system shall have a login feature based on username and password", and "The login feature shall be secure against attacks". Give three important design principles and three important implementation techniques/principles you would use to fulfill these requirements. For each principle or technique, explain why it is important in the case of this login module, and explain how you would use it.

Attacking the layer below

G3 Give a definition of what a covert channel is and give an example of a storage channel.

D3 Name two physically different types of emanations from equipment and name for each of them a type of equipment, which typically gives off this kind of emanations. Describe, in detail, for each of them, how an attack using these emanations works and what type of information is typically obtained. Please note that you need only one attack example for each type. Giving more examples or variations of your example will not give extra points.

Network security

G4 a) What is a security association in IPSec?

b) What is the role of the security policy database in IPSec?

D4 a) Explain, in detail, what DNS cache poisoning is, what the consequences of DNS cache poisoning are for those affected, and why it is so serious.

b) Explain, in detail, how DNS cache poisoning using blind spoofing can be performed.

c) Explain, in detail, how DNS cache poisoning can be performed on a wireless network.

Biometric user authentication

G5 Give a description of enrollment, verification, and identification in a biometric system. What are the shared properties and distinguishing characteristics in these three steps?

D5 Consider a biometric identifier that is used in an authentication system. Describe and motivate six distinctive requirements that should be fulfilled by the biometric identifier. Discuss these requirements for the case of a biometric identifier based on face recognition. Do not use more than one page for your answer.

Copyright protection

G6 One type of copyright protection is the preventing/obstructing techniques.

The mechanisms of copying was modeled as a comparison between risk and gain in a copying situation. Give exactly one example of a preventing/obstructing technique and describe how this example can be analyzed and understood using this model.

D6 a) Let C be a binary code with 12 codewords of length 8, and for which the minimum Hamming distance of the code is 3. Consider the feasible sets of pairs of codewords in the code. Is it possible to say anything about the size of the largest such feasible set, and in that case what can be said? Is it possible to say anything about the smallest such feasible set, and in that case what can be said?

b) We define two binary codes:

C1={ (00001),(00010), (00100), (01000), (10000)}

C2={ (00001),(00010), (00100), (01000), (10000), (00000) }

Which is the greatest c1 and c2 for which C1 is c1-frame proof, and C2 is c2-frame proof? Prove your statements!