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

Written exam
TDDC03 Information Security
2005-03-11

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 Answer TRUE or FALSE to the following statements. Motivate your answer and explain the underlined keywords.

a) The mobile code paradigms of "remote execution" and "code on demand" are essentially identical. Only the viewpoint of the observer changes.

b) All Java classes are subject to bytecode verification.

D1 Under which assumptions are the following statements TRUE. Under which assumptions are they FALSE. Explain the underlined keywords during your argumentation.

a) For an access control decision (by the Java AccessController) to succeed, every protection domain on the call stack has to have the required permission.

b) The Java Security Manager (and AccessController) base access control decisions on code source and signer.

c) A virus is a mobile agent.

Writing secure code

G2 Design principles for secure software are divided into two categories: principles for restriction and principles for simplicity. Explain how restriction and simplicity relates to code security and give examples of at least two specific design principles from each of the two categories.

D2 Race conditions are tricky both for programmers and attackers. First, explain what a race condition is and how it can be exploited. Second, describe possible race condition issues in creation and use of temporary files. Finally, give examples of how programmers can avoid race conditions in creation and use of temporary files.

Attacking the layer below

G3 In general, a "channel" is any path used by an active sender to get information across to a receiver. Give a reasonable short definition or explanation of what a "covert channel" is! This should need no more than three sentences. Also give a very short example of a covert channel!

D3 First answer the question above (G3), giving both a definition/explanation and an example! Then use this as a basis for a short discussion of the two concepts "inference" and "non-interference" in your example! Finally, give an example of when inference can be used even when there is no active sender deliberately using a covert channel!

Network security

G4 What is IPSec? What services does it provide, and how does it differ from other related protocols, such as SSL or WPA?

D4 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 that would effectively eliminate cache poisoning attacks.

Biometric user authentication

G5 What is the difference between identity verification and identification? Is there a difference in performance? Why/why not?

D5 Many countries are currently implementing biometric passports. Give at least two advantages and two disadvantages of using biometric passports. (Use at most one page for your answer.)

Copyright protection

G6 a) The lecture discussed the "mechanism of copying". Based on this mechanism it was said that copyright protection techniques can be divided into two different classes. Name the classes and describe what they mean.

b) Which of the two classes does broadcast encryption belong to? Motivate your answer!

D6 Let $\Gamma = \{w_1, \ldots w_5\}$ be a binary code defined as:
$w_1 = 000000$
$w_2 = 111000$
$w_3 = 101010$
$w_4 = 110011$
$w_5 = 001111$

Let c be the maximum integer such that it holds that Γ is c-frameproof.

a) Which is this c?

b) Prove that Γ is not c+1-frameproof.

c) Add one bit to the end of each codeword, so that the new code, Γ', is c+1-frameproof! Prove that Γ' is c+1-frameproof (possibly using previous results in this problem).