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

Written exam
TDDC03 Information Security
2006-08-09

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 Name and describe four components of the Java security architecture.

D1 Comment the following statements. Are they true, false or “it depends”? Why? Elaborate.

a) An advantage of the code-on-demand model is that the client needs not update its service.

b) The Java Sandbox is always enabled.

c) Computing with Encrypted Functions (CEF) is a countermeasure against malicious mobile code.

d) JAAS (Java Authorization and Authentication Service) bases access control decisions on the login name of the Java process owner.

e) When calling Java methods through *AccessController.doPrivileged(...)*, they are executed as trusted code without any access control checks.

f) When the security manager checks whether code signed by Alice is allowed to access the file */tmp/a.txt*, it contacts the host from which Alice's code was downloaded to verify her signature.

Writing secure code

G2 a) Describe what safety and liveness properties of code are, including how they differ.

b) What does the division into safety and liveness properties of code imply in terms of enforceable security properties and run-time detection of security attacks?

D2 Full disclosure in the context of computer security means that all details of a security vulnerability are disclosed to the public, including how to detect and exploit it. The leading argument behind full disclosure is that releasing vulnerability information results in quicker fixes and better security. Discuss pros and cons with full disclosure from three perspectives (answer separately on a, b, and c):

a) The end users’ perspective

b) The open source community's and its developers' perspective

c) The perspective of commercial companies selling closed source software

Attacking the layer below

G3 The course literature on emanations and physical tamper resistance contains a lot of material on smart cards as crypto devices. Mention two basic precautions that smart card designers should use in order to reduce the risk of successful attacks on crypto keys in such cards!

D3 In the lecture on inference, two main categories were mentioned: Database trackers and covert channels. Explain shortly what each of them is, and also explain the two major types of covert channels. Give a short example for each (one for database trackers, and one for each of the two types of covert channels)!

Network security

G4 Which are the two most important protocols in IPSec, and what security services does each of these protocols provide?

D4 Intrusion detection systems are often used to detect potential attacks on a network, but it is, and particularly in the past has been, fairly easy to evade an IDS (tricking it into ignoring suspicious traffic) by carefully constructing the packets sent to the network.

a) Explain what the underlying problem, common to essentially all IDS evasion techniques, is.

b) Suggest a realistic way to design an IDS that is not vulnerable to the problem requested in (a) above.

c) Name at least one mechanism in TCP and one mechanism in IP that might be exploitable to evade an IDS, and explain how they could be exploited to do so.

d) Name two things that a protocol designer should look for when designing a protocol, that might make the protocol vulnerable to IDS evasion.

Biometric user authentication

G5 State four distinctive requirements we have on a biometric identifier which should be used in an authentication system.

D5 You are an information security consultant and you have a customer who wants a biometric system. State six distinct and relevant questions that should be considered before recommending a biometric identifier. Your costumer wants a system that limits the entrance to an important room in her company. Approximately ten people have access and they use this room five times a day on average. Which biometric identifier do you recommend? Discuss how well your chosen method fulfills the requirements behind your initial six questions, and to what extent it fails! (No method is perfect). Do not use more than one page answering this question.

Copyright protection

G6 Explain the following techniques that hide a messages in another message:

a) Steganography

b) Fingerprinting

c)Watermarking

D6 a) Given the following code with four codewords
(1 1 1 1 1)
(1 0 0 1 1)
(0 0 1 0 1)
(0 1 1 0 0)

which groups of 2 codewords have (1 0 1 0 1) in their feasible set? Is this code 2-frameproof? Prove your answer.

b) Create a code with 3 codewords that is 2-frameproof. Prove that your code is 2-frameproof.