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

Written exam
TDDC03 Information Security
2006-06-07

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 How can agents be attacked by malicious hosts? Explain and describe shortly four countermeasures that can protect the agent.

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

a) The client-server model is a mobile code paradigm.

b) Signed code means that a piece of code presents the runtime system with a signature which contains the permissions the code needs to execute successfully.

c) Detection of malicious code can only be done with anti-virus software.

d) A Java socket permission is checked every time a Java program wants to open a network connection to another host.

e) The bytecode verifier could just as well be integrated into the Java compiler.

f) In order to read a file, an applet must have a `java.io.FilePermission “<the file>”, “read”` permission in the browser's Java policy file.

Writing secure code

G2 a) Explain the design principle of complete mediation and why it is important.

b) Explain the two conditions that must hold for a race condition to be present in a system.

D2 a) In the study on security requirements three causes for poor requirements were given -- inconsistency in the selection of requirements, inconsistency in level of detail, and almost no requirements on standard security solutions. Explain how the local heroes phenomenon relates to one or more of these causes.

b) Are functional or non-functional security requirements more common according to the study mentioned above? What may be the causes of this relationship?

c) Give two examples of functional security requirements and two examples of non-functional security requirements. Formulate your examples as full requirement statements.

Attacking the layer below

G3 Explain in just a few sentences what a database tracker is, and why there is no absolute defense against it, as long as some users can use statistics commands on fields where they are not allowed to read the individual values.

D3 Suppose that as a security consultant, you should demonstrate how the value of a system crypto key in a smart card can be found by a user, who owns a card belonging to the system. Name three different general attack methods that might be tried. Then select the method that you would prefer, and describe in more detail what resources you need in terms of equipment and knowledge and how these resources are used in the attack!

Network security

G4 Explain what a trust relationship is (avoid circular explanations such as "when A trusts B there is a trust relationship" -- you need to explain what is meant by "trust"), and why trust relationships are an important concern in network security.

D4 TCP SYN flooding is a remote denial of service attack that can be launched against any TCP server.

a) Explain what TCP SYN flooding is, and how it results in a denial of service attack.

b) What is the general design flaw in TCP that makes this attack possible? Explain it in general terms that would apply not only to TCP but also to other protocols with similar flaws.

c) Show how to design the initial handshake in such a way that SYN flooding (or similar attacks) become infeasible. Explain your design in detail. It must be functional as well as secure. Explain how and why it differs from TCP.

Biometric user authentication

G5 Name two differences between an authentication system with biometric identifier and an authentication system with password.

D5 Consider the following biometric identifiers and for each suggest an application (scenario) where it is suitable. Discuss the advantages and disadvantages of each identifier in its scenario.

a) voice

b) fingerprint

c) DNA

Do not use more than one page for your answer.

Copyright protection

G6 Name and explain two of the tracing properties mentioned in the lecture.

D6 In a binary fingerprinting system there are two codewords, or fingerprints, a = (00100) and b = (10010).

a) List all fingerprints in the feasible set for a and b if erasures are not allowed.

b) Give two codewords that together with a and b give a 2-frameproof code (with four codewords). Prove that it is 2-frameproof.