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

Written exam
TDDC03 Information Security
2005-06-07

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 a) Describe briefly the concept of proof-carrying code (PCC). Mention who does what and whether PCC is suitable in all situations or not.

b) What is JAAS (Java Authorisation and Authentication Service)?

D1 Under which assumptions are the following statements TRUE. Under which assumptions are they FALSE. Define keywords that are underlined. Explain specific terminology that you use.

a) Code signing prevents attacks by malicious mobile code.

b) The Java Security Manager prevents that a malicious Java application accesses the file system.

c) The following policy file implies that example.jar signed by Eve has full control over the computer:

```
grant codebase "file:/tmp/example.jar", signedBy "eve" {
   permission java.io.FilePermission "<<ALL FILES>>", "read, write";
};
```

Note the underline marks within the policy file that denote that you should explain what is underlined.

Writing secure code

G2 To succeed with an intrusion or to "hijack a computer system", an attacker needs to perform two steps. Explain these two steps and give an example of an attack form where you highlight how these two steps are carried out.

D2 To prevent intrusions the system producer can use static (= compile time), and/or dynamic (= run time) prevention techniques. Describe at least two strong points and two weak points of each kind of technique. Give an example of a static tool and a dynamic tool, and explain how they prevent intrusions.

Attacking the layer below

G3 Give a short example of how you can get secret information like an encryption key from a smart card without physically damaging the card and without failure of the actual access control instructions on the card!

D3 Explain what SAT noninterference, Shared Resource Matrices, and Information Flow Analysis have in common and how their respective approaches differ! Note that no detailed description of each of the three entities is needed, just an overview of a few lines on how each of them treats the basic problem, and what main shortcomings they have.

Network security

G4 List the most important improvement in WPA over WEP and state why it was introduced. State one very serious limitation in the security provided by all of WEP, WPA and 802.11i, and state at least one possible consequence of this limitation.

D4 a) Explain how cookie-based handshakes work, and explain the main advantage(s) of cookie-based handshakes over how standard TCP and many other protocols perform handshakes during connection setup.

b) TCP SYN cookies provide TCP with cookie-based handshakes, but the way the cookie is encoded and transmitted limits the functionality of the TCP connection. How is the SYN cookie transmitted? Why was that particular method chosen? What limitations does the use of TCP SYN cookies place on the TCP connection? When might it be (and when isn't it) appropriate to use TCP SYN cookies?

Biometric user authentication

G5 Briefly explain a problem which can occur if the
a) universality
b) acceptability
c) circumvention
d) permanence
requirement is not met by a biometric system. Tackle each missing requirement one at a time so in total you will describe four different problems.

D5 Consider the following biometric identifiers and for each identifier suggest an application (scenario) where it is suitable. Explain why this identifier is suitable in this particular application. Also give some disadvantages that apply to the selected application. (Please use AT MOST ONE PAGE for your answer.)

a) Fingerprint
b) DNA
c) Written signature

Copyright protection

G6 Name three techniques that hide a message in another message and describe the main differences between the techniques?

D6 Below are all copies of a fingerprinted text, with three bits codewords:

(We assume that the pirates can only make changes in the positions where their copies differ and they can only choose between existing words)

```
The fantastic new technology will have profound impact on future cars.
The fantastic new technology will have great    impact on new    cars.
The amazing   new technology will have profound impact on new    cars.
The amazing   new technology will have great    impact on future cars.
```

Write a binary representation of the code.
For which greatest c, called c', is the code c-frameproof? (c is the number of colluding pirates)
Prove that the code is c'-frameproof.
Prove that the code is NOT c'+1-frameproof.