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

Written exam
TDDC03 Information Security
2005-08-11

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 with TRUE or FALSE and motivate your answer.

a) Computing with encrypted function (CEF) protects the confidentiality of a computation.

c) The Java Virtual Machine within a web browser bases access control decisions for applets on the identity of the user that owns the browser process.

D1 Describe the Java security architecture by describing the steps (in the architecture) that signed(!!) applet code must pass to access the local file /tmp/applet.txt.

Writing secure code

G2 a) Should the programmer use a model of good or bad behavior when implementing input validation? Explain why.

b) Explain the terms simplicity and restriction in the context of design principles for secure software.

D2 There are many variants of buffer overflows. The simplest variant is overflowing a stack buffer all the way to the return address, redirecting the return address to attack code. Explain and give examples of other buffer overflow variants where:

a) the attacker uses another overflow technique;

b) the overflowable buffer is in another location; and

c) the attacker aims at another target.

You should come up with three examples in total. Be as specific as possible when explaining technique, location and target, and how they affect the way the attack is carried out.

Attacking the layer below

G3 Name two physically different kinds of emissions that can reveal secret data, and give a short example for each of the two on situations where they can appear!

D3 In chapter 14.6, Ross Anderson describes seven different ways of attacking smart cards, which do not rely on emissions. Recall at least three of these attacks from the text or the lecture, and describe them in no more then half a page each!

Network security

G4 A company has a sensitive network of computers on an isolated network. The network is not accessible from the outside through any channels at all and the company has complete control over what is connected to the network and who does the connecting. Because of this, they don't bother to keep services on the network updated with the latest security patches.

Explain why this is a mistake. Give an example of a *realistic* scenario in which the lack of security updates could be a serious problem, and possibly result in a breach of security.

D4 Explain the concept of a "trust relationship", in the context of network security and explain why trust relationships are so important in network security.

Give two dissimilar examples of trust relationships that might exist in a real system, and clearly explain their potential impact on the security of the overall system.

Biometric user authentication

G5 a) Multimodal biometrics can be of two types. Briefly describe these two types!

b) Describe one advantage and one disadvantage of using multimodal biometrics! (As opposed to using biometrics in the "ordinary" way.)

D5 a) How is the false match rate (FMR) of a biometric verification system related to the FMR (called FMR_N in Maltoni et al.) of the same biometric system used for identification? Clearly state all assumptions you make.

b) How is the false non-match rate (FNMR) of a biometric verification system related to the FNMR (called $FNMR_N$ in Maltoni et al.) of the same biometric system used for identification? Clearly state all assumptions you make.

c) How do the above relations affect the scalability of identification systems?

Copyright protection

G6 Answer true or false to the following statements:

a) Watermarking embeds different marks in each copy.

b) In steganography the existence of a hidden message should be secret.

c) Fingerprinting is only used on decryption keys.

d) Steganography is a deterring technique, i.e. increases the risk to be found.

e) Similar embedding techniques can be used in watermarking and fingerprinting.

D6 A pirate knows that the fingerprinting code look like this:
(We assume that the pirates can only make changes in the positions where their copies differ and they can only choose between existing words)

```
0001
0010
0100
1000
0000
```

The pirate also has the following three texts:

```
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.
```

a) Give one example of a text that the pirate can create and use illegally without being caught.
b) Is the code 2-frameproof? Prove your answer.