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

Written exam
TDDC03 Information Security
2007-03-10

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.

Writing secure code

G1 a) Explain the implications of the quote "Security features are not secure features".

b) Is the following true "Execution monitoring can only enforce security policies specifying safety properties of code"? Why or why not?

D1 a) Explain what a format string attack is and how it works.

b) The run-time tool Stackguard protects against buffer overflow attacks. How would you design a run-time protection against format string attacks? Explain your assumptions. Give at least one drawback of your technique. Your design should be on a technical level. Software with your run-time protection should only interact with the end user by sending reports of potential attacks to the system administrator.

Running code securely

G2 a) Name two elements of the Java security architecture and explain them shortly.

b) Anti-virus software can use a variety of strategies to detect malicious code. Name and explain one strategy.

D2 a) Explain the meaning of the following policy file.

```
grant codeBase "http://www.ida.liu.se/~kim/code.jar", signedBy "kim" {
        permission  java.io.SocketPermission "www.isy.liu.se:80","connect, resolve";
}
```

Specifically do not forget to explain how Kim's signature is verified.

b) What is the advantage of running a piece of code as privileged code? Choose an example and elaborate.

c) Name and explain two strategies used by malicious code for hiding from detection.

Network security

G3 Network Address Translation (NAT) is sometimes abused as a security mechanism. Explain at least two reasons why NAT is not sufficient to protect a networked computer.

D3 Some firewalls have a feature called "connection tracking". When this is activated, the firewall stores information about the state of every network connection through the firewall, which allows fine-grained control over traffic filtering.

a) Having connection tracking enabled creates a security vulnerability not present when connection tracking is off. Explain what that vulnerability is, how connection tracking causes it, and how it can be exploited.

b) A similar vulnerability exists in certain network protocols. Name at least one

such protocol, and explain, in detail, how such a protocol can be designed to avoid this vulnerability.

Identity management

G4 Explain what single sign-on (SSO) is. Briefly describe how SSO is achieved in Microsoft Passport and in Liberty Alliance. What are the main similarities and differences between the two systems?

D4 All phishing attacks fit into the same general information flow. At each step in this flow, different countermeasures can be applied to stop phishing.

a) List and briefly describe each of these steps. Use these steps to describe a concrete phishing attack.

b) Select three steps from your list at point (a). For each of these steps present one countermeasure that can block the attack in that step. Explain each countermeasure and discuss its advantages and disadvantages. How can these countermeasures prevent the attack you described at point (a)?

c) Which are, in your opinion, the main causes that make possible phising attacks? Discuss three causes.

Biometric user authentication

G5 "You can change your password, but you cannot change your fingerprint." Answer the following questions:

a) What is the technical term for the core problem addressed in this statement?

b) Give a more general description/definition of this problem (be as precise and concise as possible)

c) Why is this problem so important, i.e., what are its consequences?

D5 a) Draw a picture that displays the generic architecture of a biometric authentication system. Make certain your architecture picture contains all biometric system components as presented in the lecture and identifies which components communicate with each other over interfaces.

b) Given the architecture you drew in part (a), specify which components (and in which order) are used for user enrollment.

c) Given the architecture you drew in part (a), specify which components (and in which order) are used for user identity verification.

d) If you were to augment this architecture to allow for multiple method authentication, where would this functionality go?

Attacking the layer below

G6 The first part of "the layer below" treated inference and transmissions of data between strict confidentiality classification levels. One major technique for this is database trackers and another is covert channels. Describe very briefly (no more than one written page for the whole question) what these two techniques are and give a short, simple example for each!

D6 Physical probing is one way to get protected information out of a smart card. But there are other ways in which for example a pay-TV customer may get the crucial system key out of card without resorting to removing any physical casing etc. Describe at least two different attacks of this non-intrusive kind! Just their names will not give any points. At least an attempt at a proper description is required.