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

Written exam
TDDC03 Information Security
2004-04-19

Permissible aids
Dictionary

Teacher on duty
Claudiu Duma, 013-281790 or 073-9073213.

Instructions and points

There are 8 general questions and 8 in-depth questions. The general questions are from G1 to G8, and the in-depth questions are from D1 to D8. The questions are grouped pair-wise under their corresponding topic.

You have to answer at most 4 general questions and 4 in-depth questions. You should choose only one question from each topic, so that it will be 4 (general) + 4 (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 4 points from general questions and 12 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 4 (general) + 4 (in-depth) questions we will randomly choose 4 + 4 answers for correcting the exam, while the rest of the answers will be discarded.

Risk Analysis

G1 Explain the keywords asset, threat, vulnerability, and safeguard. Name three examples for each as found in the risk assessment of a software company.

D1 A small IT company approaches you to help them with a risk assessment of their business. They have recently lost their customer database due to a hardware failure and missing backup routines. In addition a senior developer had to be fired because of personal problems and has vowed (promise) to bring the company down. The company is very worried.

Help them with a risk analysis identifying assets, threats, vulnerabilities, risks and safeguards. State assumptions about costs and risks but *focus exclusively on the problems mentioned in this text*. What safeguards do you suggest and how do you motivate the safeguard costs?

Evaluation standards, e.g. Common Criteria

G2 The Common Criteria (CC) provides a standardized framework for stating security requirements, and it allows for two constructs into which security requirements can be collected to a security requirements specification: 'Protection Profiles' (PP) and 'Security Targets' (ST). Explain the difference between a PP and an ST in the way they are used. What are the two different types of security requirements in CC?

D2 Explain the relation between evaluation criteria, evaluation methodology and a scheme. Which are the three main user groups of the Common Criteria, except accreditors, and in what way can each one of them benefit from the CC (what is the intended use of the CC for the different user groups)?

Copyright protection

G3 Give two reasons why the problem of illegal copying is worse now than 20 years ago.

D3 Shortly describe fingerprinting, watermarking, and traitor tracing (technical detail is not needed). Point out differences and similarities and give examples of situations when the different techniques can be used.

Mobile code security

G4 Trusted hosts and trusted hardware are two defense mechanisms for protecting the mobile code from malicious host. Explain what are the similarities and differences between the two mechanisms. Shortly describe how they work and what security properties they achieve. Compare their advantages and disadvantages.

D4 The evolution of worms is influenced by a number of aspects. For instance, one such an aspect is the *common platforms and software*. As discussed by Darrell Kienzle and Matthew Elder, worm creators are looking to exploit vulnerabilities of *common platforms and software*, thus assuring a high rate of spreading for the worms. Enumerate and shortly describe four other aspects considered by the authors to have an impact on the evolution of worms. Discus in greater details two of the aspects you have mentioned.

Attacking the layer below

G5 Emissions are normally associated with electromagnetic radiation that can be picked up by radio-type receivers. But there are lots of other signals that may reveal sensitive data to someone intercepting them. Name at least two other types of emissions, including a situation for each where they can be used! (The chosen situation should be specific enough to indicate what is required for an attacker to be able to take advantage of the emission.)

D5 Smart cards are often used for such purposes as encryption or signing of short messages. Describe at least three different attacks to reveal the key from a card that you hold! All attacks should use entirely different phenomena and the basic descriptions should be more detailed than just a word or expression in order to be counted at all.

Security in IEEE 802.11 Wireless Networks

G6 Explain the WPA key hierarchy. For each key in the hierarchy, explain what it is used for, from what information it is computed and why that particular information is used.

D6 WEP is vulnerable to at least two passive attacks that allow an attacker to read all encrypted frames. WPA is not.

a) Explain, in detail, two passive attacks against WEP that result in the attacker being able to read all encrypted frames.

b) Explain, in detail, how WPA prevents these attacks.

Building secure software

G7 a) What is a race condition, why can it be a security vulnerability, and how can a potential attack look?

b) Explain the principle of minimizing the attack surface. Also give three short, practical examples of what it could mean.

D7 Explain how a buffer overflow attack works (preferably in both pictures and text) and fit the attack form into the two crucial steps of an intrusion. Present at least three different ways of preventing this kind of attack. Analyze the differences in the three prevention techniques and try to find pros and cons.

Biometric user authentication

G8 Explain briefly the following requirements on a biometric identifier:

a) distinctiveness

b) permanence

D8 At a university campus a student run cafe is serving coffee at a reasonable (low) price.

Since a lot of students want to have a cup of coffee during the short breaks between lectures a long line of people is often formed. Currently everyone wanting to buy coffee needs to pay cash to the cashier. At a board meeting it is discussed how to speed up the service. The plan is to sell prepaid coffee credits and perform user authentication using biometrics when a student wants a cup of coffee.

Suggest a biometric identifier which can be used, and explain why it is a good idea to use this identifier. Can you see any problems with your suggested solution?

One of the persons at the meeting asks what the advantages and/or disadvantages would be of using a multi-modal biometric system. How would you answer him/her?