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

Written exam
TDDC03 Information Security
2004-03-06

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.

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 Define qualitative and quantitative risk analysis. What are advantages and disadvantages? Under which circumstances would you choose a *qualitative* risk analysis?

D1 You have developed a freeware e-mail client. Prior to letting people use it you want to perform a risk assessment of it so you can be reasonably assured that you have released a reliable piece of software.

a) What risk assessment methodology do you choose? Why? Elaborate on whether you use a qualitative, quantitative or mixed approach.

b) Exemplify the process of risk assessment by describing a small but complete part of the risk assessment of your e-mail client.

Evaluation standards, e.g. Common Criteria

G2 You are a product developer that has decided to evaluate your product according to the Common Criteria. The product is still in its specification phase. There are evaluated Protection Profiles (PP) for the type of product/system you are developing. Describe a relevant question you should pose when deciding to which, if any, PP you whish to make Claims in the Security Target (ST) for your product.

D2 A user has purchased an IT-product which has been evaluated at, what in the context can be considered, a high level of assurance. After some time in use, the product, to the user's dissatisfaction, suffers a security breach. Explain to the user what is gained by a security evaluation, and motivate why it needs not necessarily be considered as wasted, even though the product apparently still contains exploitable vulnerabilities. (Hint: the question is concerned with "assurance" in relation to "security".)

Copyright protection

G3 a) The lecture discussed the "mechanism of copying". Based on this mechanism it was said that copyright protection techniques can be divided into two different classes. Which?

b) For each of the following copyright protection techniques, decide which of the two different classes it belongs to.

1. Fingerprinting
2. Macrovision
3. Secure Platforms

D3 Book's Franchising Corporation (BOFINC) will release their first publication; a book called "Creating Novels Using Technology (CNUT)", about writing literature on word processors. They are fully aware of the risk of this book being illegally copied and want to minimize this risk.

1. Describe fingerprinting in general. What problem can be solved, and how is that achieved?
2. Show how the general description in 1 applies to the specific situation of BOFINC.

Mobile code security

G4 What are the two major security problems in mobile code security? Give an example for each of the two problems.

For each of the following defense mechanisms listed below state what it protects against.

a) Proof carrying code
b) Trusted hardware
c) Sandbox
d) Computing with encrypted functions

Pick two of the mechanisms from the list above and shortly describe how they work.

D4 A mobile agent is sent by a user to visit a number of travel bureaus in order to find the best flight to a certain destination. When finding the best offer, the mobile agent should book and pay for the flight and then return to the user. What are the security problems in such an application scenario? Consider both the possibilities of malicious agent and malicious travel bureau. Analyze the security requirements from both the agent's user point of view and from a travel bureau point of view? Propose a realistic security solution (possibly combining different defense mechanisms) to address the security requirements you have found. Analyze the possible limitations or disadvantages introduced by your security solution. You should state your assumptions and motivate your choices.

Attacking the layer below

G5 Describe what a covert channel is and how it is related to the concept of different levels in the computer ("Level" here refers to such levels as hardware, OS-kernel, general OS support etc., not to security levels).

D5 Choose any of the more detailed attacks described in the recommended advanced literature by Ross Anderson (or any similar attack you have knowledge of from another source). Describe what happened in as few sentences as possible, not more than half a page with normal handwriting. Then point out what was the basic design weakness, what the defense is, or, if there is no known defense, why there cannot be one, and finally point to similar weaknesses in other situations, if there are any.

Security in IEEE 802.11 Wireless Networks

G6 a) Explain how AES-CCMP works.

b) Why does WPA use Michael instead of a proven cryptographic hash function such as MD5 or SHA-1?

D6 A denial-of-service attack on WPA is possible where the attacker sends frames with invalid MICs to an access point less than one minute apart. Because of the countermeasures used to compensate for the short MIC, the access point will keep invalidating its keys before without ever being able to renegotiate them. In practice, the only way to perform this attack is to perform a man-in-the-middle attack against the channel between a station and the AP.

a) Explain why this attack is so difficult to perform without resorting to man-in-the-middle.

b) Explain, in detail, how to perform the attack as a man-in-the-middle attack.

Building secure software

G7 a) Explain the principle of least privilege and describe at least two security problems related to this principle.

b) Explain why we need to validate input, and mention at least two rules of thumb when implementing input validation.

D7 A very important thing to understand is what Michael Howard and David LeBlanc try to stress by saying "*Security features* are not *secure features*". Explain what they mean, and give extensive examples of what *security features* are, what *secure features* are, and how they can be combined to secure a system with several computers connected to the Internet. Consider various forms of threats against the system and how these threats can be mitigated with security features, secure features, or both. (Be clear on which things are security features and which are secure features.)

Biometric user authentication

G8 a) What is the difference between identification and identity verification?

b) Give examples (one for each case) of the use of biometrics for:
- positive recognition
- negative recognition

D8 In a few months, everyone who wants to enter the United States will be required to either have a passport with some biometric data or a visa. Some biometric identifiers might be better for this purpose than others. Explain why or why not the following biometric identifiers are appropriate to use in passports: Iris, DNA, gait (=how a person walks). What security problems are there? What privacy problems are there?