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

Written exam

TDDD17 Information Security

2008-03-08

This exam is **only** for the students who are registered for **TDDD17**.

There is a separate exam for TDDC03 Information Security.

Make sure you have the right exam!

Permissible aids

Dictionary (printed, NOT electronic)

Teacher on duty

David Byers, 0708-282821

Instructions

There are 5 general questions and 5 in-depth questions. The general questions are from G1 to G5, and the in-depth questions are from D1 to D5. 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 must answer at least one of the questions for each topic. 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.

Attention

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.

Hardware and Operating System Security

G1 A common schema is to classify security mechanisms into "Deter, Detect, Alarm, Delay, and Respond". Map the concept of tamper evident and tamper responsive onto those, and describe how the two categories provide the security mechanism you mapped them to. Give one example for each of the two.

D1 Assume you are the system administrator of a Unix/Linux system that had been broken into with a buffer overflow attack. The attack happened analogous to the procedure shown in the lecture.

a) Suppose the attacker has just done his exploit (e.g., he has a root shell on your system) but not yet changed anything in your system. Is it possible for you as the administrator to discover the attack? If yes, which tracks could the attacker remove to prevent you from discovering him, and how?

b) Suppose the vulnerable program was run with the rights of a very restricted user, for example one who has no rights to access files in the directory /bin. Would the mentioned buffer-overflow attack still work? If yes, would there be a way to avoid this attack without changing anything in the program code? If no, where would this attack fail?

File System Security and Trusted Computing

G2 Assume you have to build a computer system that stores the launch codes of nuclear missiles, and provides them only to authorized users. What certification requirements would you impose (either expressed as TCSEC or Common Criteria). Would you prefer to store this information on paper instead? Why / why not?

D2 If you were do design an encrypting file system, how would you manage keys? Per file? Per User? Propose a solution and give your design considerations.

Identification and Authentication

G3 The IEEE Computer journal contains in its February 2008 issue a paper where two multi-method user authentication systems are compared: Smart cards with PIN and cards with manually checked hand-written signatures. One interesting point in their analysis is that they obviously do not take into account that chip card systems should not perform passive read out of static card parameters when using PINs. But apart from that, they still notice that PINs may be worse

than signatures simply because PINs can be easily observed by people close by, while it is more difficult to learn how to imitate a handwritten signature.

The study takes into account only one of the two types of error possibilities for a biometric system. What are the two error types? Apply them to PINs, and write down what a user must or can do to avoid them! Will any precaution against one type influence the rate of the other, as it always does in biometrics? Then also mention what differences you would expect for both error rates between a manual check of signatures and an automated check! Motivate your opinions clearly in both the discussion on PINs and the one on handwritten signatures!

D3 The text describes seven different requirements on a biometric identifier. Compare fingerprints to passwords using these requirements! What is the crucial one among these requirements that after all makes fingerprints preferable from a strict security point of view? Also point out which of the requirements that you regard as the second most important for biometrics from a pure security point of view and motivate your choice!

Network Security

G4 Name the three main protocols in IPSec and state what security functions each protocol provides.

D4 Many network protocols, particularly older ones, do not fully specify behaviour under all conditions. For example, the IP specification does not specify how to handle overlapping fragments.

Explain why this kind of situation is a problem in general from a security point of view and give at least one concrete example (other than IP fragments) where a network protocol is incompletely specified, and describe the concrete security consequences in that example.

Risk Analysis, Business Continuity Planning, Physical Security

G5 What is the typical output of (a) a risk analysis, (b) a hazard analysis, (c) business continuity planning?

D5 a) Describe a hazard analysis method of your choice.

b) Name and “very shortly” describe the phases of business continuity planning. Which phase do you consider most important? Why?

c) Name two Google search strings that can provide valuable information to a hacker. What information is provided and why is that information valuable?