LiTH, Linköpings tekniska högskola

IDA, Department of Computer and Information Science
Ulf Kargén

Written exam
TDDD17 Information Security
2023-08-18

Permissible aids
English dictionary (printed, NOT electronic)

Teacher on duty
Ulf Kargén, ulf.kargen@liu.se, 013-285876

Instructions
There are 4 main questions on the exam. Your grade will depend on the total points you score. The maximum number of points is 32.

Since the number of credits for the exam have changed from 3 to 2 hp (or ECTS) in 2020, we use two different grading scales depending on which year you were admitted to the course, as shown in the table below. *Make sure to fill in the correct Module (TEN1/2/3) on the exam cover sheet.* The grading scales are preliminary and might be adjusted during grading.

Grade	C (3)	B (4)	A (5)
Points required **TEN2 (3 hp)** Students admitted **2019 or earlier**	19	24	27
Points required **TEN3 (2 hp)** Students admitted **2020 or later**	16[1]	22	26

[1]And to those of you who would like to point out that 16/19 > 2/3, I say that the number of points you score on the exam is not a linear function of how many hours you studied.

1. System Security (8 points)

a) All modern CPUs have a special-purpose instruction used to perform system calls. How does this special instruction work, and what is the security rationale of this design? (2 points)

b) In a typical OS, data in RAM belonging to different processes is strictly isolated.

   i. Explain why this is necessary in order to enforce access control in an OS. (1 point)

   ii. Explain how this isolation is achieved. Be sure to clearly explain the hardware and software mechanisms involved. (2 points)

c) Explain the design principle *Separation of privilege* (as defined by Saltzer and Schroeder), and give an everyday example of how this principle is used in modern IT systems. (2 points)

d) With the traditional access control mechanism used in Unix/Linux, one can assign read/write/execute permissions to owner/group/others. What access control scheme (among the ones discussed in the course) is this an example of? What characterizes this method for access control? (1 points)

2. Defense against Malware (8 points)

a) *Polymorphism* and *metamorphism* are two classical techniques used by malware authors to bypass antivirus scanners.

   i. Which detection method do these circumvention techniques target? Why are they able to circumvent the detection method? (1 point)

   ii. As a response to these circumvention techniques, antivirus providers came up with a complementary detection approach. Name it, briefly explain how it works, and how it helps to defeat polymorphism and metamorphism. (2 points)

b) Consider the problem of classifying binaries as either benign or (potentially) malicious. In the course, we discussed two types of *supervised* machine learning for this task. What are those called, and which of them would be most suited for detecting *advanced persistent threats*? Motivate your answer. (2 points)

c) Malware have traditionally been divided into *viruses, worms*, and *trojans*. Today, almost all malware are trojans. Explain why. (3 points)

3. Network Security (10 points)

a) What are trust relationships in the context of computer networks? Give examples for a university network. (2 points)

b) Describe the evolution of WiFi security from WEP to WPA3. (4 points)

c) Describe the taxonomy of different types of Intrusion Detection Systems (IDS). (4 points)

4. Privacy (6 points)

a) Describe in your own words how the Mixnet communication method guarantees anonymity and what are its limitations. (2 points)

b) What is the privacy challenge in statistical databases? Also, briefly explain the various statistical disclosure control approaches. (2 points)

c) When it comes to counting-queries, the query results are perturbed by adding a random number (noise) to it in order to achieve the differential privacy guarantee. How to calibrate the noise that is added to the query results? (2 points)