LiTH, Linköpings tekniska högskola

IDA, Department of Computer and Information Science
Ulf Kargén

Written exam
TDDD17 Information Security
2022-08-19

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) Pick two of Saltzer and Schroeder's secure design principles, and for each of the two, name and describe the principle and give a practical example of where it is applied. (4 points)

b) In a sentence or two, explain the concept *Root of Trust* (RoT). (1 point)

c) Explain how the two technologies Intel SGX and ARM TrustZone differ in terms of the RoT (i.e., what is the RoT, and why). (2 points)

d) Consider a multi-user system, where different users might not completely trust each other. From a security perspective, which of the following two technologies would be preferable for isolating different users from each other: *virtual machines* or *containers*? Briefly motivate your answer. (1 point)

2. Defense against Malware (8 points)

a) Explain the difference between *signatures* and *heuristics* in antivirus products. (2 points)

b) Third-party antivirus products are frequently used on desktop or laptop computers, but are less common on mobile platforms (Android or iOS). Explain the main technical reason for this. (1 point)

c) Explain how *emulation* in combination with *static signatures* can be used to defeat (i.e., detect) *packed* malware. Why are static signatures alone not sufficient? (2 points)

d) Consider the two problem statements (i) and (ii) below. Among the three machine-learning (ML) types *classification, clustering*, and *anomaly detection*, which would be best suited to solve each problem? Motivate your answer by, for each problem statement, briefly discussing how suitable *each* ML type would be for solving the problem, and pick the best-suited one. (3 points)

i. Using ML as an aid for manually dividing a set of malware samples into different families.

ii. Building an ML-based HIDS (Host-based Intrusion Detection System).

3. Network Security (10 points)

a) There are several different kinds of firewalls. Explain what characterizes the following kinds of firewalls, and briefly discuss the pros and cons of each type. (2 points)

   i. Packet filter

   ii. Stateful firewall

   iii. Application layer firewall

b) Describe main principles used in cellular network security (2G/3G/4G). What has changed from generations to generation? What are common attacks attempted in cellular systems? (4 points)

c) Suppose you are running an Intrusion Detection System over IPv4 traffic. (4 points) What kind of packet fields (e.g., destination IP address) can you use for traffic analysis (i.e., those are not encrypted) if the flow is using:

   i. TLS 1.2

   ii. IPsec transport mode ESP

   iii. IPsec tunnel mode AH

4. Privacy (6 points)

a) For some applications and services, identification of subjects is necessary, e.g., authentication services. Explain the privacy property that enable a system to identify a subject in a privacy friendly manner. (2 points)

b) Explain the two types of privacy risks in statistical databases. (2 points)

c) Explain the intuition of the Differential Privacy definition with an example. (1 point)

d) One way to achieve ε-differential privacy guarantee for counting queries, is to add carefully calibrated noise (number) to the query results. Explain, in your own words, why adding any random number to the results will not give us privacy protection. (1 point)