LiTH, Linköpings tekniska högskola

IDA, Department of Computer and Information Science
Ulf Kargén

Written exam
TDDD17 Information Security
2023-03-23

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) Explain what is meant by *attestation* in the context of trusted computing. (1 point)

b) Consider an e-identity solution running as a mobile app (such as Bank ID). Explain one concrete reason why your bank might would want to perform remote attestation of your mobile device (if it was possible) prior to letting you log in to your internet bank with the e-identity. (1 point)

c) Many modern programs, such as PDF readers and web browsers, utilize sandboxing to reduce the attack surface of software exploits. The complex rendering logic executes with minimum privileges, while privileged operations are mediated and carried out by a much smaller software component. This design embodies two of Saltzer and Schroeder' secure design principles. Name and explain these two principles, and explain how they are applied in the above context of software sandboxing. (4 points)

d) Assume that an attacker has managed to install a bus snooping device in a computer system, which allows him/her to continuously read all data flowing on the memory buses. Explain why Intel SGX could be used to mitigate such an attack, while a software-only memory encryption scheme could not. Clearly motivate your answer based on the technical characteristics of Intel SGX. (2 points)

2. Defense against Malware (8 points)

a) Explain the reasons (discussed in the course) why antivirus products are increasingly using cloud-based detection. (4 points)

b) Briefly explain one approach mobile apps could use for detecting if they are being run in a sandbox. (1 point)

c) The set of permissions is usually considered a more robust feature for mobile malware detection than properties of the (byte)code of an app. Briefly explain why. (1 point)

d) Consider the following approach for evaluating a machine-learning based malware detector: first, a large dataset consisting of 50% malicious and 50% benign binaries are compiled. The dataset is constructed in such a way that it is representative of current in-the-wild malware, and currently in-use benign programs. Next, the detector is tested on this dataset, and the accuracy is found to be 99%. Clearly explain why this information is insufficient for deciding if the detector could be deployed in practice. What additional information would be needed? (2 points)

3. Network Security (10 points)

a) What information can port scanning give? What are common methods? (2 points)

b) Compare the security architecture and protocols in WiFi networks versus cellular (3G, 4G) (4 points)

c) Describe behavior vs knowledge-based IDS. Which is better to handle encrypted traffic? (4 points

4. Privacy (6 points)

a) Explain in your own words the minimum anonymity guarantee that an anonymous communication system provides to its users? Further, write down the various privacy guarantees that technologies that ensure "hard privacy" strive to achieve (2 points)

b) Explain, in your own words, two risks to users' private information in an identity management system and give a brief account of a privacy enhancement technology that mitigates those risks (2 points).

c) Explain in your own words the unlinkability guarantee in the context of database systems, considering the two linkability risks that arise in database systems (2 points)