LiTH, Linköpings tekniska högskola

IDA, Department of Computer and Information Science
Ulf Kargén

Written exam
TDDD17 Information Security
2022-06-07

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. 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) Assume that a disk-encrypted computer has been left powered on, but with the screen lock active (so that you need to provide a password to access the user interface).
   i. Name and explain *two* possible attacks mentioned in the course, which could be used to read out the data on the encrypted disk. Assume that the attacker has physical access to the computer. For each attack, briefly explain all steps of the attack. (4 points)
   ii. For each of the two attacks in (i), explain why or why not ARM TrustZone would be able to protect against the attack. (1 point)
   iii. For each of the two attacks in (i), explain why or why not Intel SGX would be able to protect against the attack. (1 point)

b) If the password file `/etc/passwd` cannot be read on a UNIX system, for example due to a disk problem, typically no users can log in anymore. Which of Saltzer and Schroeder's secure design principles is this an example of? In a more general context, briefly motivate the rationale for this design principle. (2 points)

2. Defense against Malware (8 points)

a) Explain what an *exploit kit* is, and how it works. (3 points)

b) *Packing* is an evasion technique frequently used by malware authors. How does it work, and what is the purpose of using it in malware? (2 points)

c) Briefly explain how an attacker might (attempt to) get a malicious app past the automatic vetting process used for Google Play apps. (1 points)

d) Suppose that we use the following procedure to evaluate a machine-learning-based Android malware detector: first, all apps from some third-party app store are downloaded, and then we use a collection of antivirus (AV) products to label each app as malicious or benign (e.g., using the majority vote among all AV products). Finally, we use this dataset to measure the accuracy of our detector. Explain why the result might be quite misleading. (2 points)

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) Which steps are typically involved in an attack on a system that is not directly accessible to an attacker? For each step, name and briefly explain one security mechanism that could be used to prevent, detect or mitigate that step of the attack. If no mechanism is applicable at one or more of the steps, explain why. (4 points)

c) DNS cache poisoning (4 points)

   i. DNS cache poisoning is a potentially very serious attack. Explain what the consequences of a successful DNS cache poisoning attack could be.

   ii. Cache poisoning is possible due to a flaw in the DNS protocol. Explain what this flaw is, and propose a way to prevent DNS cache poisoning (at least in practice, in situations where the attacker is unable to examine the DNS query). State what would be required for your solution to be deployed in practice.

4. Privacy (6 points)

a) Establish the relationship between the anonymity and unlinkability properties, then briefly describe a privacy enhancing technology that guarantees both the properties. (2 points)

b) First, describe your understanding of the "record linkage" privacy risk with an example, and then describe a way to mitigate the mentioned risk. (2 points)

c) The re-identification protection offered by the *k*-anonymity model is quite limited. Explain at least one limitation of the *k*-anonymity model and then describe how the Differential Privacy (DP) model mitigates the risk. Further, in your own words, write down the intuition of the Differential Privacy definition. (2 points)