LiTH, Linköpings tekniska högskola

IDA, Department of Computer and Information Science
Ulf Kargén

Written exam
TDDD17 Information Security
2023-06-05

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) Contrast the traditional security ring architecture with that of ARM TrustZone (2 points)

b) Consider the two attack techniques *cold boot attacks* and *DMA attacks*.

   i. Briefly describe the two techniques. How are they similar, and how do they differ? (2 points).

   ii. Imagine that your goal (as an attacker) is to learn about someone's financial situation by obtaining confidential information from the victim's e-banking service. Assume that the e-banking service uses some form of 2-factor authentication (e.g., a security token or a mobile electronic ID) for logging in to the web page. Which of the two techniques (cold boot attacks and DMA attacks) would represent the *easiest route to achieve the goal*? Clearly explain why your choice is better than the alternative one, and include a conceptual explanation of how the complete attack (i.e., obtaining financial information) would be carried out.
   (2 points)

   iii. DMA attacks are made possible due to a design decision that violates at least one of Saltzer and Schroeder's secure design principles. Pick the *one* design principle whose violation you think most strongly contributes to the vulnerability. Name that principle, briefly explain it, and explain how it is violated in the context of DMA attacks. (*Note: Answering with more than one principle will lead to a reduction of points!*) (2 points)

2. Defense against Malware (8 points)

a) Malware creation kits:

   i. From the point of view of an antivirus provider, briefly explain the "classical" process for updating client defenses when a new piece of malware was discovered, *before* the advent of malware creation kits. (1 point)

   ii. How has the emergence of malware creation kits challenged the above approach? (1 point)

   iii. Briefly explain how *unsupervised* machine learning could aid in dealing with these challenges. (1 point)

   iv. Briefly explain how *supervised* machine learning could aid in dealing with these challenges. (1 point)

b) Drive-by downloads:

   i. Explain what a drive-by download attack is. (1 point)

   ii. Explain how such an attack is typically carried out. Your answer should outline all steps in a successful drive-by download. (3 points)

3. Network Security (10 points)

a) How does one access the sites of the DarkNet? Why are those difficult to track? (2 points)

b) Does Network Address Translation (NAT) provide any additional security features, and if so, how could those be breached? (4 points)

c) Much of Internet security, especially e-commerce, is based on TLS/SSL. (4 points)

   i. What is the difference between those two?

   ii. What are certificates? How are those used and validated, and what are possible problems?

   iii. Describe, in two sentences each, five basic attacks prevented by proper use of TLS/SSL.

4. Privacy (6 points)

a) When it comes to privacy preserving techniques for communications and access management, what are the two general ways to achieve accountability while maintaining anonymity? (2 points)

b) Data privacy is highly dependent on the context (i.e., knowing whose privacy is in question); explain in your own words the concepts *respondent privacy* and *owner privacy*. (2 points)

c) What is the role of *function sensitivity* (i.e., the sensitivity of a query) in achieving ε-differential privacy guarantee? (2 points)