LiTH, Linköpings tekniska högskola

IDA, Department of Computer and Information Science
Ulf Kargén

Written exam
TDDE62 Information Security: Privacy, System and Network Security
2024-03-21

Permissible aids
English dictionary (printed, NOT electronic)

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

Instructions
There are 4 main assignments on the exam, corresponding to the topics (1) *OS security and trusted computing*, (2) *malware defense*, (3) *network security*, and (4) *privacy*. For each grade, there is both a per-assignment and a total score requirement, as detailed in the table below. The maximum number of points is 32.

The grading scales are preliminary and might be adjusted during grading.

	OS security and TC	Malware defense	Network security	Privacy	Total
For grade 3	4	2.5	4	2.5	18
For grade 4	4	2.5	4	2.5	24
For grade 5	7	4	7	4	27

1. System Security: OS Security and Trusted Computing (10 points)

a) Consider a computer system that must be shared between users that may not entirely trust each other. It can be argued, based on one of Saltzer and Schroeder's design principles, that it is better to give each user a separate virtual machine running on the system, rather than simply creating a regular user account for each user. Which principle, and why? (**Note**: your answer should include **one design principle only**. Answering with more than one principle will result in a reduction of points.) (2 points)

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

c) For each of the two hardware security extensions below, explain whether it would still be possible to trust a security mechanism based on that extension *if an attacker has managed to compromise the BIOS/Boot ROM of the computer*. (3 points)

   i. ARM TrustZone

   ii. Intel SGX

d) An *arbitrary code execution vulnerability* is a flaw in a piece of software that allows an attacker to "trick" a running program into executing (arbitrary) code supplied by the attacker. Consider an arbitrary code execution vulnerability in the following two kinds of software:

   i. A system service running with superuser privileges
   ii. A device driver

   Which of the two cases has the biggest potential impact on security? Clearly motivate your answer. (2 points)

e) Explain what Platform Configuration Registers (PCRs) are, in the context of the TPM. What is their purpose? What is the set of operations that can be performed on them, and why? (2 points)

2. System Security: Defense against Malware (6 points)

a) Briefly explain what *packing* is in the context of malware defense. (1 point)

b) In the course, we discussed two different approaches AV software might use to defeat packing. Name these, and explain how they work and how they are able to defeat packing. (3 points)

c) Consider an attempt at creating a machine-learning based detector for *advanced persistent threats* (APTs). Explain why overfitting would likely be a significant problem in this case. (2 points)

3. Network Security (10 points)

a) What are typical components of a SCADA network? Which attack methods are possible in such networks, and why? (4 points)

b) Describe the role of honeypots and how those can be used to secure a corporate network. Where (in which network zone) should honeypots be located, and why? (3 points)

c) What are the security implications of using NAT in a mixed IPv4/v6 network? Does it have any negative effects? (3 points)

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) Explain in your own words how does the K-anonymity model protect the published tables against record linkage attacks? (2 points)

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

d) Describe in your own words the risk that multi-party computation protocols help to minimize in a federated learning setting (1 point).