LiTH, Linköpings tekniska högskola

IDA, Department of Computer and Information Science
Ulf Kargén

Written exam
TDDE62 Information Security: Privacy, System and Network Security
2024-06-03

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) In the past, it was common to employ a security policy that included frequent password changes for all users (e.g., every 3 months). Today this practice has largely been abandoned, since users tended to choose overly simplistic passwords when they were required to frequently memorize new passwords. Relate this to *one* of Saltzer and Schroeders secure design principles. Name and briefly describe the principle, and explain how it relates to the above. (*Note: answering with more than one principle will result in a reduction of points*.) (1.5 points)

b) Instead of frequent password changes, it is common today to use 2-factor authentication to reduce the impact of leaked passwords. (For example, combining a password with a one-time code generated by a mobile app). Relate this to another of Saltzer and Schroeders secure design principles. Name and briefly describe the principle, and explain how it relates to 2-factor authentication. (*Note: answering with more than one principle will result in a reduction of points*.) (1.5 points)

c) Explain on a technical level how a *rootkit* can hide its presence on a system from, for example, file system scans. (2 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)

e) In the context of the TPM, explain what *sealing* is, and what it is used for. Explain the main steps of the process and the technical mechanisms involved. (3 points)

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

a) Contrast *signature-based* and *heuristic-based* malware detection. Briefly explain how they work, and what the main advantages and disadvantages of each approach are. (3 points)

b) Generally, neither signatures nor heuristics are effective for detecting *advanced persistent threats*. Explain why. (1 points)

c) Both the set of permissions and the set of strings in an app are useful features for mobile malware detection. One of them could be considered more reliable than the other, however. Which one, and why? (2 points)

3. Network Security (10 points)

a) What security weaknesses exist in DNS, and how to prevent those? (3 points)

b) How are CAs used to secure HTTP traffic? What does certificate transparency mean? How are certificates revoked? (4 points)

c) Describe the 3 main principles for secure network design. (3 points)

4. Privacy (6 points)

a) For some applications and services, identification of subjects is necessary, e.g., authentication services. Describe a technique that enables a system to provide both anonymity and accountability of a subject. (2 points)

b) Exemplify the secure aggregation protocol among 3 participating entities. (2 points)

c) In a federated learning setting, what is the privacy risk that the Differential Privacy (DP) model is employed to mitigate? Also explain how the DP model helps in mitigating the risk. (2 points)