LiTH, Linköpings tekniska högskola

IDA, Department of Computer and Information Science
Ulf Kargén

Written exam
TDDE62 Information Security: Privacy, System and Network Security
2024-08-23

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) Using an example, explain how *Role-based access control* (RBAC) works. (2 points)

b) Imagine that an attacker wanted to install spyware on a laptop. Explain how the attacker would go about to achieve this via a *DMA attack*. Also explain how a DMA attack works. (2 points)

c) 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)

d) Briefly define the *Zero Trust principle*. (1 point)

e) On a high level, explain how technologies such as the TPM or Intel SGX can help in implementing the Zero Trust principle in an organization. (1 point)

f) In the context of the TPM, explain the difference between *restricted* and *unrestricted* encryption keys. What is the reason for having this distinction between two kinds of encryption keys? (2 points)

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

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

b) What is a malware *family*, and why are malware families a common phenomenon? (1 point)

c) Name a type of machine learning that can help in identifying families in a set of malware samples. Briefly explain how it works, and how it can be used for the aforementioned purpose. (2 points)

3. Network Security (10 points)

a) What does an intruder need in order to implement a connection reset attack on the TCP? (2 points)

b) Nowadays, most traffic goes over SSL and is hard to analyze for Intrusion Detection Systems. How can an IDS still be useful? (4 points)

c) Describe main principles used in cellular network security (2G/3G/4G). What has changed from generations to generation? What are common attacks attempted in cellular systems? (4 points)

4. Privacy (6 points)

a) Explain the privacy enhancing technologies (PETs) concept and briefly describe the categories of PETs. (2 points)

b) Express in your own words with an example how credentials in attribute-based credentials allow a client to privately prove its identity to a service provider. (2 points)

c) Describe in your own words how to achieve the differential privacy guarantee for answering queries resulting in real numbers. (2 points)