LiTH, Linköpings tekniska högskola

IDA, Department of Computer and Information Science
Ulf Kargén

Distance exam
TDDD17 Information Security
2021-06-07

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

Instructions
There are 3 main questions on the exam. Your grade will depend on the total points you score. The maximum number of points is 26.

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	22	24
Points required **TEN3 (2 hp)** Students admitted **2020 or later**	16[1]	20	23

Answers should be submitted through Lisam as a single PDF or ASCII text (.txt) document before the end of the exam time. Figures should be integrated into the document and *not* submitted as separate files. If you use PDF format, figures could be drawn either electronically, or by hand and scanned/photographed. If you use plain text format, you can draw ASCII art. To facilitate easier grading, it is preferred that you express formulas, pseudo-code, etc., as electronic text, and not as handwritten figures.

You are allowed to use any aid, but **all kinds of collaboration with others is strictly forbidden**. Also, **copying any part of an answer from another source will be considered plagiarism**. The questions will be checked for plagiarism and sharing of answers between students using Urkund, and any suspected cheating will be reported to the university disciplinary board. **By taking the exam, you solemnly promise to abide by the above rules.**

In the event that you experience technical difficulties with Lisam that prevent you from submitting, it is allowable to submit answers via email. However, this should only be used as a last resort if Lisam for whatever reason would stop functioning.

The home exam will not be anonymous due to the exceptional COVID-19 situation.

Ulf Kargén will be available to answer questions during the exam via email and phone.

[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) Briefly explain the main principle of DMA attacks. (1 point)

b) Consider the two technologies ARM TrustZone and Intel SGX. Would either (or both) be able to protect against a DMA attack? Explain your reasoning and also state any (reasonable) assumptions you might make. (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) In a typical OS, kernel data is strictly isolated, so that it cannot be accessed by regular processes. Explain how this is achieved. Be sure to clearly explain the hardware and software mechanisms involved. (3 points)

2. Defense against Malware (8 points)

a) Given that essentially all malware today are trojans, would you always be safe from malware if you never obtained any software or other files from untrusted sources, and never opened any email attachments? Clearly motivate your answer. (2 points)

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

c) Consider the problem of selecting which features to use for training a machine-learning method to identify potentially malicious Android apps. Discuss how useful the following sources of information would be for gathering such features, based on what you have learned about Android malware in the course (3 points):

   i. The names of all methods in the app
   ii. The constant strings used in the app
   iii. The permissions requested by the app (as specified in Androidmanifest.xml)

d) Consider the problem of classifying binaries as either benign or (potentially) malicious. In the course, we discussed two types of supervised machine learning for this task, namely *discriminative methods* and *anomaly detection methods*. Which of those would be most suited for detecting *advanced persistent threats*? Clearly motivate your answer. (2 points)

3. Network Security (10 points)

a) What are Advanced Persistent Threats (APT) and how those are different from Hacktivism? (2 points)

b) 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)

c) Suppose you are running an Intrusion Detection System over IPv4 traffic. (4 points)

What kind of packet fields (e.g. destination IP address) can you use for traffic analysis (i.e., those are not encrypted) if the flow is using:

i. TLS 1.2

ii. IPsec transport mode ESP

iii. IPsec tunnel mode AH