LiTH, Linköpings tekniska högskola

IDA, Department of Computer and Information Science
Ulf Kargén

Distance exam
TDDD17 Information Security
2021-03-24

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**	18	22	24
Points required **TEN3 (2 hp)** Students admitted **2020 or later**	15[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 15/18 > 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) Explain, using a few sentences, what an (arbitrary) code execution exploit is.
(2 points)

For each question under (b) and (c) below, briefly explain if the attack would be possible or not. Make sure to mention all relevant security mechanisms, and why or why not they are able to prevent the attack. Also, state any assumptions you might make.

b) Consider the following scenario: Alice and Bob are both logged in to the same machine, and running a few processes each. Eve sends a malicious PDF-document to Bob, which, when Bob opens it in his vulnerable PDF-viewer, results in an arbitrary code execution exploit.

i. Would it be possible for Eve's code to compromise (i.e., modify) memory owned by one of Alice's processes? (2 points)

ii. Would it be possible for Eve's code to compromise memory owned by the OS kernel? (1 point)

c) Next, consider the case that Eve uses a second-stage payload in her exploit, which performs another (successful) arbitrary code execution attack against a *device driver*.

i. Would it now be possible for Eve's code to compromise memory owned by one of Alice's processes? (1 point)

ii. Would it now be possible for Eve's code to compromise memory owned by code running in ARM TrustZone's secure world? (1 point)

iii. Would it now be possible for Eve's code to compromise memory owned by code running in an Intel SGX enclave? (1 point)

2. Defense against Malware (8 points)

a) Clearly explain why most antivirus engines today employ *emulation*. Your answer should explain which evasion technique emulation mitigates, how this evasion technique works, why it is used by malware authors, and how emulation helps to defeat such evasion attempts. (4 points)

b) Imagine that you work as a malware analyst for an AV company. Briefly explain how *unsupervised learning* could help you determine the behavioral class (ransomware, adware, spyware, etc.) of a new malware sample you receive. (1 points)

c) Android apps run on the phone as separate users, enforcing strong separation between apps. Explain what implication that has for Android malware detection. (1 points)

d) Mention *two* methods discussed in the course that mobile malware authors can use to evade detection by *static signatures*. Briefly explain how each method works.
(2 points)

3. Network Security (10 points)

The page count stated together with the points for each question is to give you a better idea of the expected scope of the answer. Page counts assume 12pt single-spaced text. For reference, a typical A4 page contains about 500 words when using this text size.

a) If users are located near the same Wi-Fi Access Point, can they hear/understand each other’s traffic? What has changed in the latest standard? (3 points, 0.6 page)

b) Describe how DDoS attacks are typically performed and what are the most common protection mechanisms. (4 points, 0.8 page)

c) Describe the main methods, goals and tools for network scanning. (3 points, 0.6 page)