LiTH, Linköpings tekniska högskola

IDA, Department of Computer and Information Science
Ulf Kargén

Distance exam
TDDD17 Information Security
2021-08-20

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) Using a few sentences, explain the concept Root of Trust. (1 points)

b) Come up with a simple real-life (i.e., not computer related) example that illustrates how Role-Based Access Control (RBAC) works. Make sure that the example demonstrates all relevant properties of RBAC. (2 points)

c) All modern CPUs have a special-purpose instruction used to perform system calls. How does this special instruction work, and what is the security rationale of this design? (2 points)

d) Consider the two somewhat similar attacks *cold boot attacks* and *DMA attacks*. Based on what we have discussed in the course, compare the two and discuss pros and cons of each attack (3 points).

2. Defense against Malware (8 points)

a) Some modern OSes (for example, Windows and Mac OS) use code signing to verify the trustworthiness of executable files. When an executable is started, the OS first checks the digital signature. If the signature check fails, the executable is prevented from running. If an executable is not signed, the user is asked for confirmation before the program is allowed to run. Explain what implications this has for the three main "distribution" methods of malware discussed in the course, i.e., *viruses*, *worms* and *trojans*. (3 points)

b) How effective would code signing be to prevent *drive-by-downloads*? Clearly explain your reasoning. (2 points)

c) It is known that mobile malware is significantly more common for the Android platform than for the iOS platform. Explain why. (1 point)

d) The emergence of malware creation kits is one of the reasons why antivirus companies are increasingly using machine learning for malware detection. Explain why. (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) Does Network Address Translation (NAT) provide any additional security features, and if so, how could those be breached? (4 points)