CHALMERS UNIVERSITY OF TECHNOLOGY
Department of Computer Science and Engineering
Examination in Computer Security EDA263 (DIT641) for the International Master's Program in Computer Systems and Networks, Tuesday 5 June 2018, 14:00—18:00

Examiner: Associate professor Magnus Almgren, Ph.031-772 1702,
email: magnus.almgren@chalmers.se

Teacher available during exam: Magnus Almgren, Ph.031-772 1702

Language: Answers and solutions must be given in English.

Grades: will be posted before Friday 29 June 2018. The exam review date/place will be set individually for students since the result is reported outside of Chalmers regular academic year.

You are **not** allowed to use any means of aid.
However, according to general rules printed English language dictionaries are allowed.

Please write the answer to each question (question 1, question 2, etc) on a separate sheet of paper.

Grade: The grade is normally determined as follows:

30 p ≤ grade 3 < 38 p ≤ grade 4 < 46 p ≤ grade 5 (EDA263)

30 p ≤ pass < 46 p ≤ pass with distinction (DIT641)

1 Terminology (15p)

a) In the course, we discussed different terms, such as *vulnerability, threat, and countermeasure.* Frame an explaination of what a packet filtering firewall is, by accurately using these three terms in your answer. (5p)

b) Give an example of an *active* attacker and what s/he could do. Give an example of a *passive* attacker and what s/he could do. (2p)

c) Give two examples with a short explanation of what *boundary protection mechanisms* can be. (4p)

d) Give two examples with a short explanation of what *internal protection/recovery mechanisms* can be. (4p)

2 UNIX Security (6p)

a) Explain the commands *su* and *sudo* that you would type in a terminal window for UNIX. Also make sure your answer for each command includes an example where it would be suitable to use the one command (and where the other one would not work well). (4p)

b) A security consultant has been asked to improve the security of a UNIX system. In a public directory that most users on the system can access, she runs the following command:

```
> ls -al
-rwxr-xr-x 1 alice prj1 18721 2009-10-13 21:56 prg1
-rws---r-- 1 root root 21872 2009-10-13 21:06 prg2
```

Which program do you suggest her to concentrate her efforts on? Explain why. (2p)

3 Risk Treatment (10p)

After having carried out a risk analysis the analyst team needs to take appropriate action.

a) There are three major methods to deal with the result of the risk analysis. Please name, describe and exemplify these methods. (6p)

b) Further, the book discusses two other methods for risk treatment that are more of a preventive type. Please name, describe and exemplify these two methods as well. (4p)

(exam continued on the next page)

4 Common Criteria (10 p)

a) Explain the meaning of and the use of the concepts TOE, PP, ST, EAL? (8p)
b) Your manager wants to buy a system that has passed a CC evaluation, but asks you if the system now is 100% secure. What is your answer to your manager? What can you say about the security of this system? Discuss and motivate your answer. (2p)

5 Malware (7p)

Give a short (i.e. less than ca. 5 lines) but exhaustive description to each of the following types of archetypal malware / attack vectors. For each instance, try to give an example and make a comparison between different types where appropriate. Example answer:
The properties for Malware X are the following:… In that sense, it is different from Malware Y described in (i). An example of malware X could do …

a) polymorphic virus
b) macro virus
c) Trojan Horse
d) zero-day exploit
e) keyloggers
f) spear-fishing
g) drive-by-download

6 Misc (12p)

Give a short (i.e. less than ca. 10 lines) but exhaustive answer to each of the following questions: (The answer must include not only the function, usage, principle etc., but also the (security) context into which the object of the question would be applicable.)

a) Biometric authentication systems are becoming more prevalent (e.g. fingerprint sensors on phones). Explain why there might still be errors in such systems even though fingerprints are believed to be unique. (4p)
b) Explain briefly how *speculative execution* was used in the Spectre attack. What side-channel attack was used in this attack and how? (4p)
c) Some exploits, such as Rowhammer, allows the attacker to be able to deterministically shift a single bit on a system. How can a single bit-shift have security implications? Give an example on how the attacker would use such an attack. (4p)