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, Monday 10 June 2019, 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
The teacher will aim to physically come twice to the exam: about 60—90 minutes after the start of the exam, and about 60--90 minutes before the end.

Language: Answers and solutions must be given in English.

Grades: will be posted before Wednesday 3 July 2019. Email the teacher for setting up an exam review since Chalmers is no longer in session.

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 (9p)

The book discusses deception and lists three types of attacks that can lead this threat consequence: masquerade, falsification, and repudiation. Explain what each term means and give a practical example for each one.

The terms are described page 41.

2 Security Principles (15p)

During the course, we have discussed several important security design principles. Please (1) explain the meaning of the following and (2) give an example of a security mechanism discussed in the course and what the particular design principle could mean practically for this mechanism.

a) Cost of security versus cost of failure and recovery (3p)
b) Fail-safe defaults (default permit vs default deny) (3p)
c) Separation of privilege (3p)
d) Least privilege (3p)
e) Isolation (separation) (3p)

The terms have been discussed throughout the course. (a) partly in terms of slides module Operating System Security, L06, book page 55; (b) in terms of firewalls, etc (c) cryptography, module Security Policies (Lee, Nash, Poland), UNIX Security, authentication; (d) UNIX security, etc; (e) operating system security.

3 Passwords (5p)

In computer security, it is important to compare the opportunities and capabilities of the attacker versus the defender. For example, when it comes to system security the attacker basically just needs to find a single vulnerability to attack the system while the defender needs to patch all vulnerabilities. Sometimes the relationship of attacking / defending the system is very asymmetric between the attacker / defender.

There is a case when it comes to authentication with passwords that involves a “slow” hash where the defender can have the upper hand. Why? Explain and give an example.

Book page 97-99.

4 Operating System Security (7p)

Describe the reference monitor.

a) What is it for? (1p)
b) Name and explain at least two important requirements for a reference monitor. (4p)
c) Draw a picture showing the context in how it would be used. (2p)

Slides module Operating System Security, L06 + book page 460—462. The terms have been discussed throughout the course. (a) partly in terms of . (b) in terms of firewalls, etc (c) cryptography,

(exam continued on the next page)

5 Defensive Programming (10p)

In the lectures, we used the program snippet shown in Listing 1 to discuss attacks and defences.

a) Explain what a buffer overflow is from a general perspective. (1p)

b) Use the code shown in Listing 1 to demonstrate specifically how a buffer overflow would work. Your answer should include *a figure* of the stack when the program enters the echo function, *a description* of what the attacker would do, and *how* this affects the stack (as a second figure). (6p)

c) We discussed three main system defences against buffer overflows. ***Choose one*** of these system defences and explain how it works. Then explain in detail using the specific code from Listing 1 how an attacker might still be able to perform her attack even if the stack is protected by this particular defence mechanism. Please be concrete and include a figure of the stack in your answer. (3p)

Listing 1 (for Q5): *The network server*

```
1  char gWelcome [] = "Welcome to our system! "
2
3  void echo (int fd) {
4      int len;
5      char name[64], reply [128];
6
7      len = strlen (gWelcome);
8      memcpy (reply, gWelcome, len);
9
10     write_to_socket(fd, "Type your name: ");
11     read (fd, name, 128);
12     memcpy (reply+len, name, 64);
13     write (fd, reply, len + 64);
14     return;
15 }
16
17 void server (int socketfd) {
18     while (1)
19         echo (socketfd);
20 }
```

See "Buffer Overflow" module (slides + book Ch 10, esp. p 344). Lab 1. See L08C for defences (NX, Canaries, ASLR). L08C describes one example of an attack even if these defences are in place but others exist..

(exam continued on the next page)

6 Miscellanous Questions (14p)

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.). Each part is worth 1 point, unless otherwise stated.

a) What is drive-by-download? Give an example.
b) What is steganography? How is it different from encrypting a text?
c) Explain briefly what a ticket is in Kerberos and how it is used.
d) Explain the *side-channel attack*. Give an example.
e) What is meant by Security Target and Protection Profile? Which is the difference? (2p)
f) The Morris worm used three types of attacks. Explain two of them. (2p)
g) Explain what two-factor authentication is.
h) Should passwords be hashed? Why/why not?
i) Briefly describe the difference between DAC and MAC related to authentication.
j) What is meant by key escrow?
k) What is the focus in the deontological theory of ethics?
l) What is ransomware? Describe how it works and how you can protect yourself.

a) Example in "Malware Module"; b) Discussed in Cryptography module; c) Network Security Module; d) Malware and attacks module; e) Common Criteria ("Security Management"; f) Slides in Malware and Attacks; g) Authentication, Auth and Access Control; h) Book 97-99 plus lecture notes; i) Authentication, Auth, and Access Control module; j) Cryptography module; k) "Security Management Module"; l) book 220