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, Wednesday 26 August 2015, 14:00—18:00

Examiner: Assistant 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 Tuesday 15 September, 2015.

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:

$30 \text{ p} \leq \text{grade } 3 < 38 \text{ p} \leq \text{grade } 4 < 46 \text{ p} \leq \text{grade } 5$ (EDA263)

$30 \text{ p} \leq \text{pass} < 46 \text{ p} \leq \text{pass with distinction}$ (DIT641)

1 The Question

Propose an interesting question of your own about the course material (and include the answer). ’Knowledge’ questions (questions that aim at reproducing some material from the course material directly) may give you 5 points (max), while ’insight’ questions may give you a maximum of 10 points. In both cases, the answers have to be correct. The scoring is based on the originality of the question, the scope, and how well it would test learning of concepts from the course.

(10 p)

2 Security Models

In the course we discussed several security models. Please describe the main objectives of the Clark-Wilson model including the additions proposed by Lee, Nash and Poland. Also give a detailed example of how it can be used. Your example should demonstrate the principal components in the model.

(10p)

3 Side Channel Attacks

a) Explain the *side-channel attack*.
b) Sketch a short program that tries to protect a “secret” but would be vulnerable to a timing-based side-channel attack.
c) Exemplify your answer in (a) by showing how an attach would work against the program in (b).

(5 p)

4 Intrusion Detection

A security expert investigates the university’s (packet-based) IDS which has 99.9% accuracy. In other words, it looks at every network packet and if it is malicious, the IDS will flag it as such in 99.9% of the cases. Conversely, it will erroneously flag only 0.1% of all benign traffic as malicious. Say the campus receives about 25 million packets per day and on average one packet per day is malicious. The expert thinks for a moment and says:

“So... if the IDS raises an alarm, the probability of it being a malicious packet is about 0.4%”.

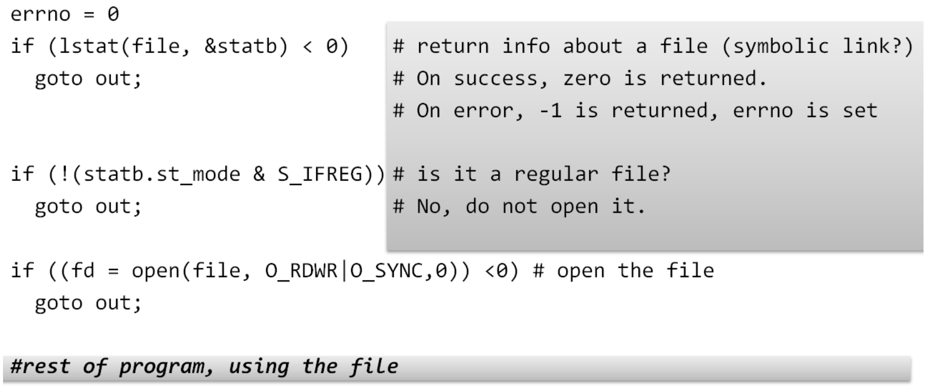
True or False? Explain your reasoning.

(10 p)

(exam continued on the next page)

5 Defensive programming

Programs running with high privileges in the system are often the target for the attacker. We discussed Kerberos and the risk of the privileged daemon opening a symbolic link instead of a regular file, as the link can point anywhere in the file system. Below is a simplified version of code from Kerberos. Explain the TOCTOU flaw and if this code is vulnerable to that type of flaw. If so, draw a figure illustrating how the attack would happen. We have added comments (# …) so that students not familiar with C also can answer.



```
errno = 0
if (lstat(file, &statb) < 0)   # return info about a file (symbolic link?)
  goto out;                    # On success, zero is returned.
                               # On error, -1 is returned, errno is set

if (!(statb.st_mode & S_IFREG))# is it a regular file?
  goto out;                    # No, do not open it.

if ((fd = open(file, O_RDWR|O_SYNC,0)) <0) # open the file
  goto out;

#rest of program, using the file
```

(5 p)

6 Miscellanous Questions

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) What is a *salami attack*? Give examples.
b) Explain the macro virus. Give an example.
c) The Morris worm used three types of attacks. Explain two of them.
d) There are two fundamentally different ways of causing a denial of service attack. Describe them and give an example for each type.
e) How does a DDoS attack differ from a DoS attack? Draw a figure.
f) What is a Trojan horse? Give examples.
g) What is a zombie?
h) What is data remanence ? Give an example how it relates to nonmagnetic media.
i) What is steganography? How is it different from encrypting a text?
j) Explain briefly what a *ticket* is in Kerberos and how it is used.
k) What is meant by computer forensics?
l) Explain what two-factor authentication is.
m) Should passwords be hashed? Why/why not?
n) What is a Man-in-the-middle-attack? What is achieved by it?
o) What is meant by key escrow?
p) Will signing a message protect its confidentiality?

(20 p)