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, Saturday March 15 2014, 08:30—12:30

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

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

Solutions: No solutions will be posted.

Language: Answers and solutions must be given in English.

Grades: will be posted before Friday 4 April, 2014.

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

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 Security and dependability concepts

a) List the main security attributes and briefly explain their meaning.
b) What protection mechanisms exists in principle if you consider threats / attacks to a system? Explain, give examples and draw an illustrating figure.

(10p)

2 Common Criteria (CC)

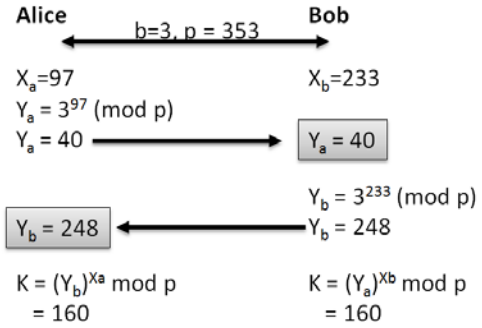
a) Explain the meaning of and the use of the concepts TOE, PP, ST, EAL?
b) Assume a system has passed a CC evaluation. What can you say about the security of this system? Discuss and motivate your answer.

(10p)

3 Cryptography

You are sitting on an airplane when you notice that the passenger next to you is correcting exams. You glance over and see the following (partial) answer from one student.

a) What algorithm is described and
b) what can this particular algorithm be used for?
c) What is the underlying assumption of why an attacker, Eve, cannot derive the key even though she sees the information exchange (marked with arrows)?



(5p)

4 Network Security: Firewalls

Below you have two sets of firewall rules. Describe the difference between them with advantages and disadvantages for each case.

action	src	port	dst	port
deny	*	*	{mail}	25
allow	*	*	{web}	80
allow	*	*	*	*

Rule Set A

action	src	port	dst	port
deny	*	*	{mail}	25
allow	*	*	{web}	80
deny	*	*	*	*

Rule Set B

(5p)

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 UNIX Security

One of the simplest way of storing passwords on a system would be to use a list with the user names and the passwords in clear text, such as in the /etc/passwd file (with other info):

username	password	user identifier	(more fields)
olle	mydogiscalledFelix!	100	...
helen	s5%d#gqqj	101	...

Any system administrator concerned with security would not use such an implementation. Explain how passwords are actually stored in UNIX systems. For each feature that adds a layer of security, explain why it is there and how it increases the protection of the passwords. Include an image where the features you described are highlighted.

(10p)

7 Malware

a) Explain what two-factor authentication is.
b) Describe in detail a plausible attack where modern malware could defeat the protection offered by two-factor authentication involving SMS.

(5p)

8 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) What is data remanence ? Give an example how it relates to nonmagnetic media.
c) What is a Trojan horse? Give examples.
d) What is a zombie?
e) What is steganography? How is it different from encrypting a text?
f) The Morris worm used three types of attacks. Explain two of them.
g) There are two fundamentally different ways of causing a denial of service attack. Describe them and give an example for each type.
h) Explain briefly what a *ticket* is in Kerberos and how it is used.

(10 p)