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 9 April 2016, 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 Friday 29 April 2016. The exam review date/place will then be posted on the homepage.

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 Personnel security

Describe how to enforce personnel security in an organisation. *What* actions need to be taken, *how* and *when*? (10p)

2 Defensive Programming

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.

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).

c) We discussed three main system defences against buffer overflows, where one was the canary. Describe the other two briefly by stating what they do and why this makes it harder for the attacker to perform the attack.

d) Explain in detail using the specific code from Listing 1 how an attacker still might be able to perform her attack even if the stack is protected by a canary. Please be concrete and include a figure of the stack in your answer.

(10p)

Listing 1: *The network server*

```
char gWelcome [] = "Welcome to our system! "

void echo (int fd) {
    int len;
    char name[64], reply [128];

    len = strlen (gWelcome);
    memcpy (reply, gWelcome, len);

    write_to_socket(fd, "Type your name: ");
    read (fd, name, 128);
    memcpy (reply+len, name, 64);
    write (fd, reply, len + 64);
    return;
}

void server (int socketfd) {
    while (1)
      echo (socketfd);
}
```

(exam continued on the next page)

3 SYN spoofing attack

Please explain the SYN spoofing attack as described in the book. Your answer should discuss the following.

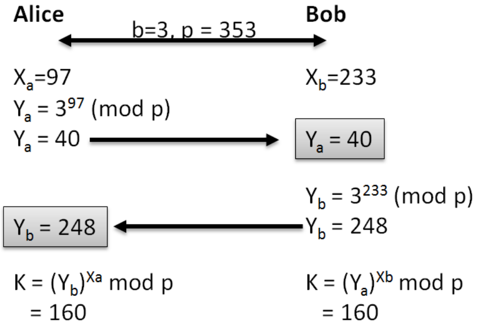
a) The normal three-way handshake of TCP connection procedure (as a figure).
b) How the attack works (use the figure from a) in your description).
c) What “weakness” of the target computer the attacker is targeting.
d) One key requirement for the attack to work (hint: what happens with RST packets?)
e) One reason why the attacker may choose this attack over a message flooding attack.

(10p)

4 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. You realize this is the Diffie-Hellman algorithm discussed in the lectures.

a) What can this particular algorithm be used for?
b) What is its the underlying security assumption?
c) What happens if the information (marked with arrows) is sent in clear text (not protected by encryption) and the adversary Eve manages to sniff the network and extract these parameters?



(6p)

5 Intrusion Detection Systems

a) Explain the principles of *anomaly detection* for an intrusion detection system.
b) Explain the base-rate fallacy by giving a numerical example. In the beginning of your answer, you should choose (and state) the accuracy of the IDS, the number of packets analyzed per day, and how many of these are malicious. Then use these numbers to give a numerical example to explain the base-rate fallacy. Show the steps in your calculations, and approximate as necessary. (10p)

(exam continued on the next page)

6 Malware

a) 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 …

i. virus
ii. polymorphic virus
iii. macro virus
iv. Trojan Horse
v. logic bomb
vi. backdoor
vii. worm
viii. zero-day exploit
ix. keyloggers
x. rootkit
xi. spear-fishing
xii. drive-by-download

(12 p)

b) Ransomware attacks has lately increased. Describe how it works, and how you can protect yourself.

(2 p)