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 19 March 2016, 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

Language: Answers and solutions must be given in English.

Grades: will be posted before Tuesday 12 April 2016.

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 A basic system model of security, dependability and their attributes

a) The course has suggested a system model for the integrated concept of computer security and dependability. The model puts security and dependability attributes into context. The model also describes the system's interaction with its users and environment, e.g. in terms of attacks and failures. Draw a figure that describes the model, and give a thorough explanation of it. (6p)

b) The model in a) is based on a binary assumption of attacks and failures. In reality the situation is more complicated. Name and describe a few more complicated assumptions that make the model more realistic. (4p)

See slides for L12 (Security Modeling), esp. slide 15-17 and slide 29.

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 by using the code shown in Listing 1. Your answer should include a description of what the attacker would do, and how this affects the stack (include a figure of the stack).

b) There are three main defences against buffer overflows. Describe each of them briefly.

c) Choose one of the defences from b) and explain in detail how an attacker still might be able to perform her attack. Please refer to the state 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);
}
```

See L7 for buffer overflows (slides + book Ch 10, esp. p 344). Lab 1. See L8 for defences (NX, Canaries, ASLR). L8 describes one example of an attack even if these defences are in place but others exist.

(exam continued on the next page)

3 Security Models

You are working for a law firm with the following eight clients:

New York Times, Bank of Scotland, Scandinavian Airlines, Bank of England, Air France, Los Angeles Times, American Airlines, Bank of Wales.

The law firm is using the *Chinese Wall Model*.

a) Draw a figure, showing how this (general) model would look in the specific example for this law firm. Show in the picture the three levels information is organized into and explain them with a concrete example.

b) Define the simple security rule formally in the following way:
Simple Security Rule: A subject S can read object O only if ...

c) Alice and Bob work for the law firm. State whether the following *read* accesses (performed in the order shown here) will be accepted or denied. Use your answer in (b) to explain your reasoning. Structure your answer in the following way:
Answer: x) Accepted/Denied, because …

1) Alice reads a document outlining which new offices will open in 2014 for Bank of Wales.
2) Alice reads a document outlining which new offices will open in 2014 for Bank of England.
3) Alice reads a document outlining which new offices will open in 2014 for Air France.
4) Bob reads a document outlining which new offices will open in 2014 for Air France.
5) Alice reads a document outlining which new offices will open in 2014 for Bank of England.
6) Bob reads a document outlining which new offices will open in 2014 for New York Times.
7) Alice reads a document outlining the yearly summary of earnings / losses for Bank of Wales.
8) Alice reads a document outlining the yearly summary of earnings / losses for Bank of Wales.
9) Bob reads a document outlining the yearly summary of earnings / losses for Bank of Wales.
10) Alice reads a document outlining the yearly summary of earnings / losses for Air France.
11) Bob reads a document outlining the yearly summary of earnings / losses for Air France.
12) Alice reads a document outlining which new offices will open in 2014 for Bank of Wales.

See L15 and book p457.

(10 p)

4 Authentication

a) Define what is meant by authentication.
b) Define what is meant by authorization.
c) Describe the four steps of an authentication procedure.
d) The information used for authentication can be of three (or potentially four) fundamentally different kinds. Describe and exemplify those.

(8 p)

See L2 and slides 3, 5, 6, book p95, 128-129, .

(exam continued on the next page)

5 Cryptography

Let's say that Alice, Bob and Charles would like to communicate *separately* with each other. That is, any two of the people in the group should be able to communicate without the third being able to read the messages. In the course we discussed (i) symmetric encryption and (ii) public-key encryption and your answer below should refer to these schemes.

a) In the course, we said that the key exchange needs to take place over a (possibly abstract) *channel X*, which then in turn needs to have a certain property depending on the encryption scheme, (i) or (ii).
   -- If Alice, Bob and Charles communicate using (i), what general property must the *channel X* have?
   -- If they are going to communicate using (ii), what general property must the *channel X* then have?
b) How many keys are needed for Alice, Bob, and Charles above using (i). How many keys are needed using (ii)? Include all types and motivate your answer. Also in your answer talk about scalability and how the number of keys grows as a function of n, where n is the number of group members.
c) Specify if (i) is commonly used to distribute keys for (ii), or the opposite. Why? Motivate! Is this a common application?
d) Explain how Bob can verify whether a certain public key really belongs to Alice in (ii). Why is this an important problem? In the course we spoke about trust and three schemes about trust to check whether a key belongs to a person. Explain these with advantages and disadvantages.

(8 p)

See L4-5: slide 11, 23,25, lab 2, slide 33-35.

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) Explain the *side-channel attack*. Give an example.
b) What is meant by Security Target and Protection Profile? Which is the difference?
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) What is meant by computer forensics?
f) Explain what two-factor authentication is.
g) Should passwords be hashed? Why/why not?

(14 p)

a) see L16 and slides
b) see L11 and slides
c) see L7, slide 5 (with details in the following)
d) See L11 and slide 9
e) see L15, slide 3
f) L2, slides + blackboard (see slide 4 mobile malware)
g) L2 discussion of passwords, book p96-99.