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 18 March 2017, 08:30—12:30

Examiner: Associate 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 Monday 10 April 2017. 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.

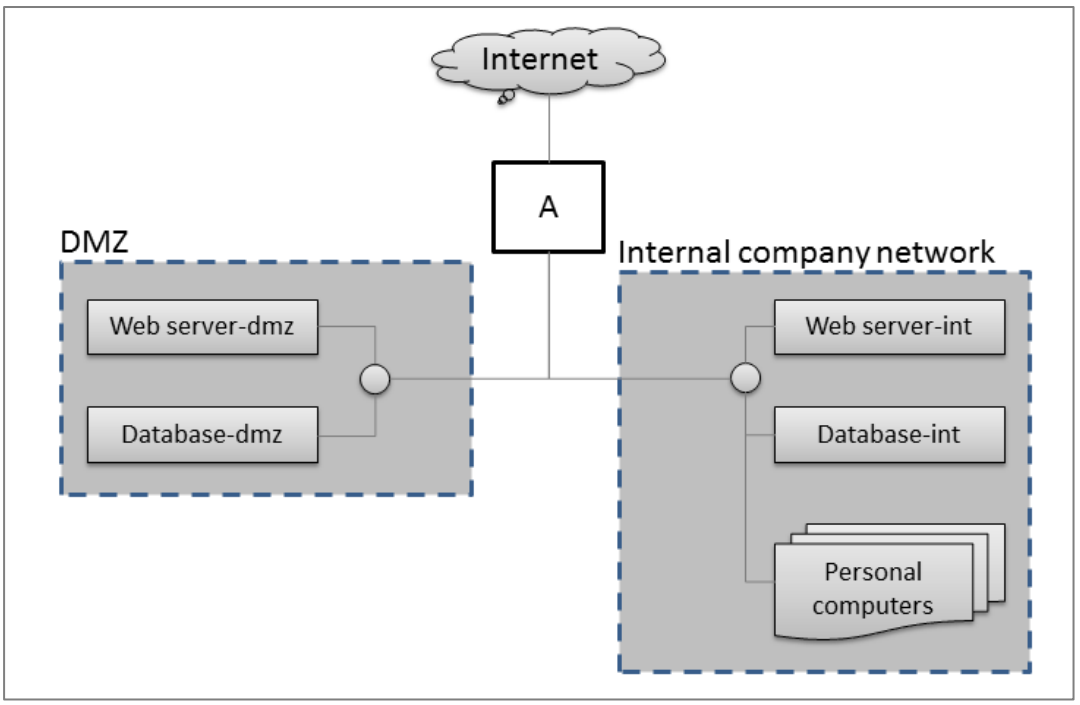
Grade: The grade is normally determined as follows:

30 p ≤ grade 3 < 38 p ≤ grade 4 < 46 p ≤ grade 5 (EDA263)

30 p ≤ pass < 46 p ≤ pass with distinction (DIT641)

1 Malware Defence (20p)

Figure 1 (for Q1)



One of your friends have just heard about attacks against databases. She would like to improve the security of her startup (shown in Figure 1) by adding a *packet-filtering firewall* in position A, but she is uncertain how effective it is against the two attacks she is especially worried about: the SQL *injection attack* and the *tracker attack* (launched by potential competitors, i.e. no insiders). **If you need to make certain assumptions, please state them clearly as part of your answer.**

Hints:
The web server of the DMZ needs to be accessed by potential customers to the company. The web server uses the `database-dmz` *to serve the web pages.*
The web server of the internal network needs to be accessed only by employees (physically located at the company). This web server uses the `database-int` *to serve web pages.*
The gray circles are simply used to denote network connection points and can be ignored.

a) Explain what a packet-based firewall is and what type of information it uses for its decision logic. Give an example rule and explain what it could do. (4p)
b) Explain what the SQL injection attack is and give an example. (4p)
c) Explain what the tracker attack is and give an example. (4p)
d) Explain how well the packet-filtering firewall positioned in A can protect systems in the DMZ against the SQL injection attacks. Be concrete and explain what type of rule you would create (use the answer for (a) to structure your answer) and how well it would work (false positives, false negatives). (4p)
e) Explain how well the packet-filtering firewall positioned in A can protect systems in the internal network against SQL injection attacks. Be concrete and explain what type of rule you would create (use the answer for (a) to structure your answer) and how well it would work (false positives, false negatives). (4p)

(exam continued on the next page)

2 Denial of Service Attacks (10p)

The book discusses two similar but different types of denial-of-service attacks: the SYN Spoofing attack and the TCP SYN Flood attack.

a) Explain the attacks separately and then discuss the difference between them and how that might influence whether an attacker would prefer to use one attack over the other. (5p)

b) In both attacks, the attacker should spoof the source address.
Give at least two reasons why. (2p)

c) If the attacker had a choice, would she choose an existing or non-existing host for the source of the attack (the spoofed address)? Motivate your answer. (2p)
   a. The SYN Spoofing attack
   b. The TCP SYN Flood attack

d) In this context, what is backscatter traffic and what can it be used for? (1p)

3 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. Describe these briefly by stating what they do and why this makes it harder for the attacker to perform the attack. (3p)

Listing 1 (for Q3): *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 }
```

(exam continued on the next page)

4 Security Models (10p)

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) What is the primary goal of the Chinese Wall Model? We are not looking for terms from the CIA, but a related concept. (1p)

b) 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. (3p)

c) Define the simple security rule formally in the following way: (2p)
Simple Security Rule: A subject S can read object O only if ...

d) 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+c) to explain your reasoning. Structure your answer in the following way:
Answer: x) Accepted/Denied, because … (2p)

1) Alice reads a document outlining which new offices will open in 2018 for Bank of Wales.
2) Alice reads a document outlining which new offices will open in 2018 for Bank of England.
3) Alice reads a document outlining which new offices will open in 2018 for Air France.
4) Bob reads a document outlining which new offices will open in 2018 for American Airlines.
5) Alice reads a document outlining which new offices will open in 2018 for Bank of England.
6) Bob reads a document outlining which new offices will open in 2018 for New York Times.
7) Alice reads a document outlining the yearly summary of earnings / losses for Air France.
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) Bob read a document outlining the yearly summary of earnings / losses for American Airlines.
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 2018 for Bank of Wales.

e) Let's add the following write accesses to the list of accesses in (d):

8.1 Alice updates (writes) to the document about outlining the yearly summary of earnings / losses for Bank of Wales. (coming after 8 but before 9).

10.1 Bob updates (writes) a document outlining the yearly summary of earnings / losses for American Airlines.

Reflect on your answer in (a), by considering the "new" accesses (7)—(11). (2p)

(exam continued on the next page)

5 Miscellanous Questions (10p)

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 meant by Security Target and Protection Profile?
   Which is the difference? (2p)
b. There are three major methods for risk treatment. Please name, describe and exemplify these methods. (6p)
c. What is a salami attack? (2p)