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 17 March 2018, 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 Tuesday 10 April 2018. 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.

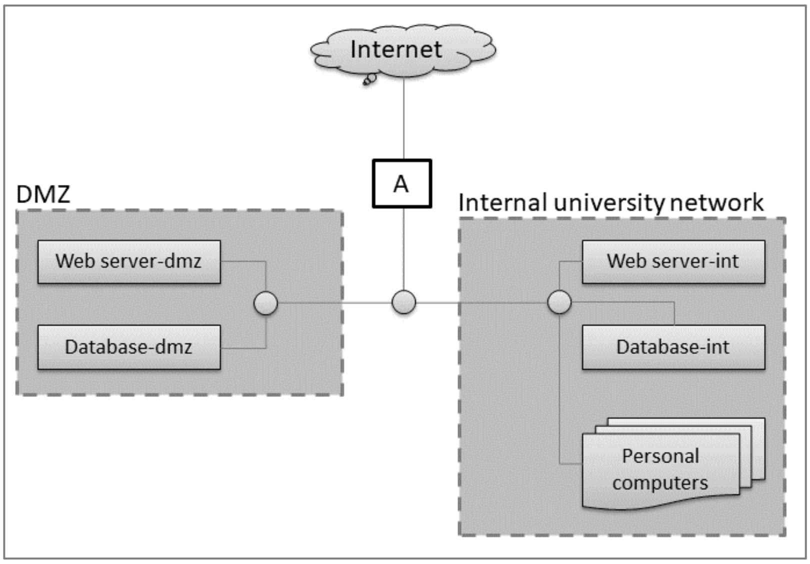
Grade: The grade is normally determined as follows:

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

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

1 Defences against attacks (20p)

Figure 1 (for Q1)



One of your friends have just heard about cyber attacks. She would like to improve the security of her university department (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 a *TOCTOU 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.**

Directions:

1. *The web server of the DMZ needs to be accessed by outsiders (potential future students). The web server uses the* `database-dmz` *to serve the web pages.*
2. *The web server of the internal network needs to be accessed only by employees/students (physically located at campus). This web server uses the* `database-int` *to serve web pages.*
3. *The computers in the DMZ are not vulnerable to the TOCTOU attack. The* `database-int/web-server-int` *is running old legacy software and might be vulnerable to a TOCTOU attack.*
4. *Important: This is a university with a low budget for security, and your friend wants to deploy a firewall (and pay for the licence)* ***only*** *if it adds security against the attacks she is worried about. That is, in your answer you need to consider the tradeoff between cost and added security. If you tell her to deploy a firewall where it does not make sense based on her concerns and the rest of the network topology, we will deduct points.*

(1 Defences against attacks cont'ed)

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. (3p)
c) Explain what the TOCTOU attack is and give an example. (3p)
d) Explain how efficient the packet-filtering firewall (positioned in A) can be in the following scenarios. Be concrete and use the answer for (a) to structure your answer. When applicable, explain what type of rule you would create for the firewall. (10p)

-- Against SQL injection attacks on the DMZ.

-- Against SQL injection attacks on the internal network.

-- Against TOCTOU attacks on the internal network.

(exam continued on the next page)

2 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. ***Choose one*** of these system defences and explain how it works. Then explain in detail using the specific code from Listing 1 how an attacker might still be able to perform her attack even if the stack is protected by this particular defence mechanism. Please be concrete and include a figure of the stack in your answer. (3p)

Listing 1 (for Q2): *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);
}
```

3 Security and dependability concepts (4p)

a) In the course, we spoke about three main security objectives. Name them and briefly explain their meaning. (3p)

b) Some in the security field feel that additional concepts are needed to present a complete picture. Name and explain one such additional concept. (1p)

(exam continued on the next page)

4 Authentication (20p)

a) Define what is meant by authentication. (1p)
b) Describe the four steps of an authentication procedure. (4p)
c) The information used for authentication can be of three (or potentially four) fundamentally different kinds. Describe and exemplify those. (3p)
d) What is two-factor authentication? (1p)
e) UNIX passwords are … (9p)
   - usually not stored in clear text. Explain what is stored and how security is improved.
   - usually combined with a SALT. Explain the SALT and how security is improved.
   - usually not stored in the file /etc/passwd. Why? What is the added security?
f) What is a rainbow table and how is this relevant to your answer in (e)? (2p)

5 Miscellaneous questions (6p)

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. (2p)
b) Explain briefly how *speculative execution* was used in the Spectre attack. What side-channel attack was used in this attack and how? (4p)