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, Tuesday 12 March 2013, 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

**Solutions:** No solutions will be posted.

**Language:** Answers and solutions must be given in English.

**Grades:** will be posted before Tuesday 2 April, 2013.

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 Metrics

a) Give at least two reasons why security is hard to measure (i.e. to assess in a quantitative way) and discuss the background for your suggestions. (2 p)

b) Suggest four possible methods to assess security (in general – thus not only specific cases such as cryptographic strength) in a quantitative way. Describe how the metric (measure) is achieved and its significance. Discuss the benefits and drawbacks for each method. (8 p)

## 2 Database Security

In the course, we discussed threats and attacks against databases.

a) Explain the nature of the inference threat to a relational database.

Consider the statistical database in Table 1 (after the question). A normal user may *not* query the database on the field "Name" and may only use formulas such as:

`count(C), sum(C,`$A_j$`), median(C,`$A_j$`), max(C,`$A_j$`), min(C,`$A_j$`), etc.`

`C` is the characteristic formula, such as *`(Sex=Male) AND (Department=Math).`*

The query set, `X(C)`, is the set of records matching the characteristic formula. $|X(C)|$ is the *number of records* in this matching set. `N` is the size of the database (number of rows or records). $A_j$ is a specific attribute, such as *`Salary`*. According to the table below, these values then give: `max(C,` $A_j$`) = 72`

b) Assume there is no other protection on the database than described above. Show the queries an attacker would use to find the exact salary of Professor Dodd, if the attacker knew that Dodd is a female CS Professor. Use `C &` $A_j$ formally in the answer you give.

c) The book describes two distinct approaches to protect the statistical database from inference attacks. The first one is *query restriction*, but describe the second technique.

d) Suppose that the *query size restriction* technique is implemented as:
$k \leq |X(C)|$, with k=2 (that is, only the lower limit is enforced).
Is it still possible to determine Dodd's salary? Motivate your answer. If it is not possible, explain why. If it is possible, show the actual queries.

e) Let's say that the query restriction is implemented with both an upper and a lower limit with k=2. Is it still possible to determine Dodd's salary? Motivate your answer in the same way as for (d).

(10 p)

Table 1: Database

| ***Name*** | ***Sex*** | ***Department*** | ***Position*** | ***Salary ($K)*** |
|---|---|---|---|---|
| Adams | Male | CS | Prof | 80 |
| Baker | Male | Math | Prof | 60 |
| Cook | Female | Math | Prof | 100 |
| Dodd | Female | CS | Prof | 60 |
| Engel | Male | Stat | Prof | 72 |
| Flynn | Female | Stat | Prof | 88 |
| Grady | Male | CS | Admin | 40 |
| Hayes | Male | Math | Prof | 72 |
| Irons | Female | CS | Student | 12 |
| Jones | Male | Stat | Adm | 80 |
| Knapp | Female | Math | Prof | 100 |
| Lord | Male | CS | Student | 12 |

**3 Risk Treatment**

a) Give a definition of risk.
b) There are two fundamentally different ways to reduce risk. Describe these two ways.
c) There are three different ways to deal with a risk that you are in fact facing. Describe the features of these three ways and their consequences. (6 p)

**4 Common Criteria (CC)**

Discuss the overall philosophy and goals behind the Common Criteria, what is achieved and how it is achieved. Describe the fundamental concepts and basic terminology. Finally, discuss the usage of the CC and potential problems and drawbacks. (10 p)

**5 Defensive Programming**

a) The function *readInput()* shown in listing 1 is vulnerable to an attack. Why? How can the function be fixed?
b) Explain what a buffer overflow is.
c) Show what a typical stack would look like if the function *readInput()* is called.
d) One defense technique is to use a *canary* on the stack. Explain what this entails and show in your picture from (c) how the stack would change.

(8 p)

Listing 1: *The function readInput*

```
void readInput(char *tag) {
    char inp[16];

    printf("Enter value for %s: ", tag);
    gets(inp);
    printf("Hello your %s is %s\n", tag, inp);
}
```

**6 Ethics**

There are two theories of ethics called the teleological theory and deontology. These may either work on an individual level or on a universal level.

a) Explain how the teleological theory works, both used on the individual level or on a more universal level.
b) Explain how deontology works, both used on the individual level or on a more universal level.

Let's look at the vulnerability reporting process. You have discovered a severe flaw in a system that controls all hydro plants in Sweden. You realize that an attacker may use this flaw to stop the production of electricity.

c) Who would you tell / not tell about the flaw? How much detail would you tell to each party? Use arguments from the teleological theory to support your reasoning. That is, we are going to grade how you applied the theory to support your answer but not the answer itself.

(6 p)

**7 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) Explain the *side-channel attack*.
c) In what context would one apply the Clark-Wilson security policy and which two concepts are enforced?
d) What is the use and goal of a honeynet? How does it function?
e) What is computer forensics? What is its relation to digital investigation?

(10 p)