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 21 March 2015, 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 Friday 10 April, 2015.

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)

The page numbers pointing to where the solutions are found in the book are based on the third edition.

1 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,Aj), median(C,Aj), max(C,Aj), min(C,Aj), 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, Aj) = 72`

b) Explain how the *query size restriction technique* can be used to protect the statistical database from an inference attack. Describe it formally using `N` and $|X(C)|$ as defined above, and the constant `k`.

c) Give a formal definition of the the *tracker attack* and describe its use in your own words.

d) Demonstrate how the *tracker attack* could be used to find the exact salary of Professor Dodd, if the attacker knew that *Dodd is the only female CS Professor*. *This is the only external information the attacker has and you cannot make any other assumptions about the values in the database.* Use `C & Aj` formally in the answer you give and list the queries used. The database is protected with the technique from (b) with `k=2.`

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	Admin	80
Knapp	Female	Math	Prof	100
Lord	Male	CS	Student	12
Major	Female	CS	Admin	80

See offprint about tracker attack as well as lecture slides.

2 Security and dependability concepts

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

b) Some in the security field feel that additional concepts are needed to present a complete picture. Name and explain two additional key concepts.

See page 33 about the CIA triad and add two more.

3 UNIX Security

A security consultant has been asked to improve the security of a UNIX system. In a public directory that most users on the system can access, she runs the following command:

```
> ls -al
-rwxr-xrwx 1 alice prj1 18721 2009-10-13 21:56 prg1
-rws---r-- 1 root  root 21872 2009-10-13 21:06 prg2
```

Which program do you suggest her to concentrate her efforts on? Explain in detail why.

See offprint about UNIX and lecture slides. prg1 = writeable by all, prg 2 = SUID but only executable by owner.

4 Cryptography

In the course, we discussed symmetric and asymmetric (public-key) cryptography. For brevity, we will abbreviate them as SC and AC. For each of the following statements, state if you agree with it and explain your reasoning. ***Note: we will not accept only yes/no answers.***

a) Asymmetric cryptography (AC) is more secure from cryptanalysis than symmetric encryption (SC).
b) AC is a general-purpose technique that has made SC obsolete.
c) AC is in general faster than SC.
d) Key management is more manageable with AC compared to SC.
e) Non repudiation can easily be achieved with SC.
f) When receiving a message encrypted with an asymmetric algorithm, you know that if you can successfully decrypt the message using the private key, no one has tampered with the message and it comes from the stated sender.
g) *Signing* a message will protect its confidentiality.
h) PGP is a symmetric system.
i) To protect the confidentiality of a very sensitive document, one should use RSA instead of AES if the key length is 256 bit.
j) In public-key cryptography (as opposed to symmetric cryptography), one has two different keys. Is it possible to use one key as a primary key and the other as a backup if the first key is lost?

See book p75 (a,b,c,d), book 76-77 + lecture slides and class (e,f,g), lab material + slides (h), slides (i,j)

5 Side Channel Attacks

a) Explain the *side-channel attack*.
b) Sketch a short program that tries to protect a "secret" but would be vulnerable to a timing-based side-channel attack.

See lecture notes about side-channel attacks

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.

See offprint for theories and example cases

7 Intrusion Detection

A security expert investigates the university's (packet-based) IDS which has 99.9% accuracy. In other words, it looks at every network packet and if it is malicious, the IDS will flag it as such in 99.9% of the cases. Conversely, it will erroneously flag only 0.1% of all benign traffic as malicious. Say the campus receives about 25 million packets per day and on average one packet per day is malicious. The expert thinks for a moment and says:
"So... if the IDS raises an alarm, the probability of it being a malicious packet is about 0.4%".

True or False? Explain your reasoning.
See slides for IDS for a calculation example

8 Risk Treatment

After having carried out a risk analysis the analyst team needs to take appropriate action.

a) There are three major methods to deal with the result of the risk analysis. Please name, describe and exemplify these methods.
b) Further, the book discusses two other methods for risk treatment that are more of a preventive type. Please name, describe and exemplify these two methods as well.

See slides L12, slide 21 or book 2nd - 528-529, 3rd - 526-527