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, Wednesday 27 August 2014, 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 16 September, 2014.

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 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`.

(8 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	Admin	80
Knapp	Female	Math	Prof	100
Lord	Male	CS	Student	12
Major	Female	CS	Admin	64

2 Network Security: Firewalls

Below you have two sets of firewall rules for incoming traffic at a company. Describe the difference between them with advantages and disadvantages for each case.

action	src	port	dst	port
deny	*	*	{mail}	25
allow	*	*	{web}	80
allow	*	*	*	*

Rule Set A

action	src	port	dst	port
deny	*	*	{mail}	25
allow	*	*	{web}	80
deny	*	*	*	*

Rule Set B

(4p)

3 Authentication using Kerberos

Below is found a somewhat simplified version of the steps in a Kerberos v.4 authentication procedure. In this, the client (C) is using the Kerberos authentication server (AS) to access a service from the server (V).

(1) C => AS: $ID_C \,||\, ID_{TGS} \,||\, TS_1$
(2) AS => C: $E_{K(C)}\,[K(C,TGS) \,||\, ID_{TGS} \,||\, TS_2 \,||\, Lifetime_2 \,||\, Ticket_{TGS}]$

(3) C => TGS: $ID_V \,||\, Ticket_{TGS} \,||\, Authenticator_C$
(4) TGS => C: $E_{K(C,TGS)}\,[K(C,V) \,||\, ID_V \,||\, TS_4 \,||\, Ticket_V]$

(5) C => V: $Ticket_V \,||\, Authenticator_C$
(6) V => C: $E_{K(C,V)}\,[\,TS_5 + 1]$

(7) $Ticket_{TGS} = E_{K(TGS)}\,[K(C,TGS) \,||\, ID_C \,||\, AD_C \,||\, ID_{TGS} \,||\, TS_2 \,||\, Lifetime_2]$
(8) $Ticket_V = E_{K(V)}\,[K(C,V) \,||\, ID_C \,||\, AD_C \,||\, ID_V \,||\, TS_4 \,||\, Lifetime_4]$
(9) $Authenticator_C = E_{K(C,TGS)}\,[\,ID_C \,||\, AD_C \,||\, TS_3\,]$

Describe briefly the following elements in the procedure and explain their function:

a) (2), $E_{K(C)}$
b) (2), K(C,TGS) and (7), K(C,TGS)
c) (2), $Lifetime_2$ and (7), $Lifetime_2$
d) (6), $TS_5 + 1$

(8p)

4 SYN spoofing attack

Please explain the SYN spoofing attack as described in the book. Your answer should discuss the following. (10p)

a) The normal three-way handshake of TCP connection procedure (as a figure).
b) How the attack works (use the figure from a) in your description).
c) What "weakness" of the target computer the attacker is targeting.
d) One key requirement for the attack to work (hint: what happens with RST packets?)
e) One reason why the attacker may choose this attack over a message flooding attack.

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 (as a figure).
d) One defense technique is to use a *canary* on the stack. Explain what this entails and show in your figure 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 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 possible 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.
   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.

(10 p)

(exam continued on the next page)

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) Explain the *side-channel attack*. Give an example.
b) Explain what a Trojan Horse is and what can happen if the compiler on the system is in reality a Trojan horse.
c) What is meant by Security Target and Protection Profile? Which is the difference?
d) What is SQL injection? What is accomplished with it? Describe what makes SQL injection possible (in principle) and how to protect against it.
e) Should one use RSA or AES to protect the confidentiality of a very sensitive document, if one knows the largest key length that can be used is 256 bit.
f) 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?

(12 p)