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 28 August 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 17 September, 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 Personnel security

It is well known that security in a company could not only rely on technical features, but "soft" and human factors play an important role. Discuss the concept personnel security from this viewpoint. Give examples of relevant security methodology related to personnel and the different phases of an employment. (10p)

2 Security and dependability concepts

a) List the traditional security and dependability attributes/aspects.

b) Group the attributes in protective and behavioural, where applicable. Explain their functionality and relation to the object system. Draw an illustrating figure.

c) Explain the interaction between attacks, vulnerabilities and failures and the object system in terms of its protective and behavioural attributes. (8p)

3 Cryptography

Let's say that Alice, Bob and Charles would like to communicate *separately* with each other. That is, any two of the people in the group should be able to communicate without the third being able to read the messages. In the course we discussed (i) symmetric encryption and (ii) public-key encryption and your answer below should refer to these schemes.

a) In the course, we said that the key exchange needs to take place over a (possibly abstract) *channel X,* which then in turn needs to have a certain property depending on the encryption scheme, (i) or (ii).
If Alice, Bob and Charles communicate using (i), what general property must the *channel X* have?
If they are going to communicate using (ii), what general property must the *channel X* then have?

b) How many keys are needed for Alice, Bob, and Charles above using (i). How many keys are needed using (ii)? Include all types and motivate your answer. Also in your answer talk about scalability and how the number of keys grows as a function of n, where n is the number of group members.

c) Specify if (i) is commonly used to distribute keys for (ii), or the opposite. Why? Motivate! Is this a common application?

d) Explain how Bob can verify whether a certain public key really belongs to Alice in (ii). Why is this an important problem? In the course we spoke about trust and three schemes about trust to check whether a key belongs to a person. Explain these with advantages and disadvantages.

(11 p)

4 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 picture, 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 works 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 how you reason.

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)

5 Authentication using Kerberos

Below is 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)

6 Software Security

When users login to a site, their credentials are checked by accessing a database with the following code, where `iUserID` and `iPassword` are two variables set by the user trying to login to the site.

```
query =     “SELECT userid from tUsers where
            userid=’” + iUserID + “’AND
            password=’” + iPassword + “’”;
```

(example of the) User Credential Database tUsers:

UserID	Username	Password	Name
1	admin	$#kaoeFor	Admin
1824	jsmith	demo1234	John Smith

From the course, you know that passwords should be stored as salted hash values to make it more difficult to perform dictionary attacks or extracting the passwords if you are an insider.

However, in this particular example, the actual code is also vulnerable to attacks.

a) What is the name for such attacks?
b) Give a (concrete) example on how the code can be misused.
c) Discuss mitigation strategies.

(6p)

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 what the "no-write-down" property means in Bell-LaPadula. Give an example why it is important.
b) Suggest an overall method that would reduce commercial spam messages and motivate why your method should work.
c) Where in the system (e.g. in which system layers) do you suggest that security should be enforced? Motivate your answer.
d) Describe the term Reference Monitor.
e) Describe the term Trusted Computing Base (TCB). What is the relation between the TCB and the “TOE Security Function” (TSF) in the Common Criteria.
f) What is meant by an organisational security policy?
g) What is the benefit of Incident handling and what is the goal with it? (7p)