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 18 January 2014, 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

Solutions: No solutions will be posted.

Language: Answers and solutions must be given in English.

Grades: will be posted before Friday 7 February, 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 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 in the case above using (i)? How many keys are needed using (ii)? Include all types and motivate your answers. 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 described three schemes about trust to check whether a key belongs to a person. Explain these schemes with advantages and disadvantages.
e) Generally, would schemes based on (ii) be more secure from cryptanalysis attacks than schemes based on (i)? Motivate your answer.

(13 p)

2 Authentication

a) Define what is meant by authentication.
b) Define what is meant by authorization.
c) Describe the four steps of an authentication procedure.
d) The information used for authentication can be of three (or potentially four) fundamentally different kinds. Describe and exemplify those.

(8 p)

3 Defensive programming

The program on the last page of the exam (vlnPrg.cc) has at least two major security problems. (Note: the password is short and in cleartext for practical reasons. This is not one of the intended problems that we are asking for.) Answer the following questions after reading the code (and the descriptive comments).

a) Explain briefly the two problems and how a hacker could exploit them.
b) Explain how the program could be fixed, i.e. give us the pseudocode that replaces lines in the original program (only for the two major problems).
c) The problems within the program has to do with a larger concept. Explain this concept.

(6 p)

4 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.

(8 p)

5 The Bell-La Padula security model

a) In the Bell-La Padula security model, two properties characterize the flow of information. Give a mathematical description of these two properties.

Now consider the following situation at an antivirus company. The following three people are employees at the company:

- Aron, cleared for (Top Secret, {Sweden, Vulnerability})
- Caleb, cleared for (Secret, {Vulnerability})
- Kate, cleared for (Confidential, {Vulnerability})

There are at least three compartments at the company: {Sweden, Vulnerability, Malware}.
Furthermore: "Top Secret" (TS) > "Secret" (S) > "Confidential" (C) > "Unclassified" (U)
Each employee keeps his/her own working diary classified in accordance to their clearance. Thus, Kate also uses the document D_{Kate}, classified as
(Confidential, {Vulnerability})
For each of the following examples, specify (1) what kind of document access is allowed (read/write/both/none) and (2) why that is so, i.e. in your answer we want you to refer to your answer in (a). For example: "only write access is allowed, read access breaks property X"
Hint: *The Security Level (L,C) dominates (L',C') if and only if* $L' \leq L$ *and* $C' \subseteq C$.

b) Aron wants to access D_1, classified as (TS, {Sweden, Malware})
c) Kate wants to access D_2, classified as (C, {Malware})
d) Caleb wants to access D_3, classified as (C, {Vulnerability})
e) Aron wants to access D_4, classified as (C, {Sweden})
f) Aron wants to access D_5, classified as (TS, {Sweden,Vulnerability, Malware})
g) Kate wants to access D_6, classified as (S, {Vulnerability}) (10p)

6 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
-rwx r-x r-x 1 root root 18721 2009-10-13 21:56 prg1
-rws --- r-x 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. (5p)

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 meant by Security Target and Protection Profile in Common Criteria? Which is the difference?
b) What is a *salami attack*? Give examples.
c) The Morris worm used three types of attacks. Explain two of them.
d) Explain briefly what a *ticket* is in Kerberos and how it is used.
e) Explain the principles on *anomaly detection* for an intrusion detection system.

(10 p)

```
#include <stdio.h>
#include <string.h>
#include <stdlib.h>
#include "processControlFcns.h"

// The following is a small part of a very sensitive
// program used to modify the temperature of a chemical process
// in a water cleaning plant. Sometimes the process is too warm
// and the process needs to be cooled. Two externally defined
// functions are used
//    int readTemperature()
//        returns the current temperature of the process
//    void lowerTemperature1Degree()
//        lowers the temperature one degree
// This program is accessible via a web interface, but it is protected
// by a secret password. To lower the temperature several degrees, we
// call lowerTemperature1Degree() through a loop. This function should
// never be called more than 9 times in a row because then the system
// breaks and the water is no longer cleaned.


int convertToNum(char chr) {
// convert character chr to a number using the underlying ASCII
// encoding. Each character is encoded using the ASCII-code, so a '0'
// is coded as 48, a '1' as code 49, an 'A' as code 65 etc.
// return -1 if an error occurrs


  int num = -1;

  if (chr>47 && chr<58) {
    // chr is a CHAR = printable letter where
    // code 48= numerical 0;code 57=numerical 9
    num = chr-48; // num is an INT containing the corresponding number
  }

  return num;
}

int main(void) {
  char secret[] = "pa33";
  char usrName[6];
  char usrPassword[9];
  char lowerTempChr[2];
  int  lowerTemp;

  // check if user is authorized to run program
  printf("Enter username:");
  gets( usrName );
  printf("Enter password:");
  gets( usrPassword );
  if ( strcmp( usrPassword, secret ) !=0 ) {
    printf("You are not allowed to run this program\n");
    exit(1);
  }
  printf("Current temperature of process is %d degrees\n", readTemperature());
  printf("Enter degrees to lower temperature (0—9):");
  gets(lowerTempChr);
  lowerTemp= convertToNum(lowerTempChr[0]); // only convert first char

  printf("The temperature will now be lowered one degree at a time, for a total of %d degrees.\n", lowerTemp
);
```



```
  while (lowerTemp != 0) {
    printf("Lowering temperature by one degree (%d)\n", lowerTemp);
    lowerTemperature1Degree();
    lowerTemp = lowerTemp -1;
  }

  printf("Current temperature of process is %d degrees\n", readTemperature());
  printf("Operation has now finished. Bye!\n");
  return 0;
}
```