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 April 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 8 May, 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)

1 Security and dependability concepts

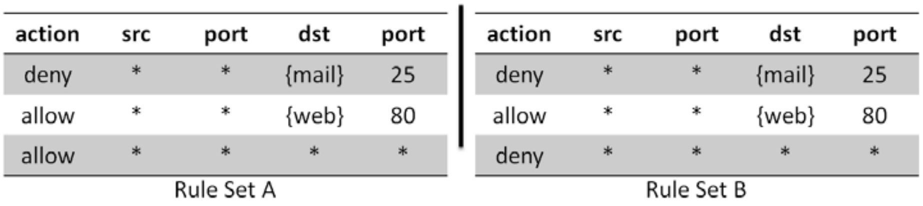
Explain the following ways of categorising attacks briefly. Give a brief example of each type.

a) Active attack
b) Passive attack
c) Insider attack
d) Outsider attack

See page 39 in book, as well as page 44.

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

See page 329-330 as well as lecture slides about firewalls.

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
-rwsr-xrwx 1 root  prj1 32721 2009-10-13 21:56 prg3
-rws---r-x 1 root  root 21870 2009-10-13 21:06 prg4
```

Rank the order she should look at these programs and motivate in detail why.

See offprint about UNIX and lecture slides. prg3 = writeable SUID. prg1 = writeable by all. prg4 = normal SUID; prg 2 = SUID but only executable by owner.

4 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.

See slides about Defensive Programming and book page 386.

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.

Lab 1, slides about buffer oveuflows, Chapter 10

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

In the course we discussed several security models. Please describe the main objectives of the Clark-Wilson model including the additions proposed by Lee, Nash and Poland. Also give a detailed example of how it can be used. Your example should demonstrate the principal components in the model.

See slides about Security Policies and Models for a detailed example, as well as book page 455.

7 Common Criteria (CC)

a) Explain the meaning of and the use of the concepts TOE, PP, ST, EAL?
b) Assume a system has passed a CC evaluation. What can you say about the security of this system? Discuss and motivate your answer.

See slides and book page 473-

8 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) 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.
d) 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?
e) What is meant by system latency when speaking about security and dependability?

a) Slides about side channel attacks
b) Page 218
c) Slides about Cryptology
d) Slides about Cryptology
e) Slides about modelling and metrics