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 2019, 14:00—18:00

Examiner: Associate 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 Wednesday 19 September 2019. The exam review date/place will be announced on the home page when the grades have been posted.

You are **not** allowed to use any means of aid.
However, according to general rules printed English language dictionaries are allowed.

Please write the answer to each question (question 1, question 2, etc) on a separate sheet of paper.

Grade: The grade is normally determined as follows:

$30 \text{ p} \leq \text{grade } 3 < 38 \text{ p} \leq \text{grade } 4 < 46 \text{ p} \leq \text{grade } 5$ (EDA263)

$30 \text{ p} \leq \text{pass} < 46 \text{ p} \leq \text{pass with distinction}$ (DIT641)

1 The Question (10 p)

Propose one interesting security-related question of your own inspired by the course material (*and provide an answer*). “Knowledge” questions, which aim at reproducing some material from the course material directly, may give you up to 5 points, while “insight” questions may give you up to 10 points. In both cases, the answers have to be correct. The scoring is based on the originality of the question, the scope, and how well it would test learning of concepts from the course. You will get no points by using variants of questions included in this exam.

No direct section in the course as questions can be made on any. Best inspiration would be from previous exams (but direct copied questions are not original and will not get a high score).

(10 p)

2 UNIX Security (10p)

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
     -rwx--x--x 1 root  root 21870 2009-10-13 21:06 prg2
     -rws---r-- 1 root  root 21872 2009-10-13 21:06 prg3
     -rwsr-xrwx 1 root  prj1 32721 2009-10-13 21:56 prg4
     -rws---r-x 1 root  root 21870 2009-10-13 21:06 prg5
```

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

Discussed in Lecture 2 (Unix security), and in Offprints (section 1).
prg1 writable by anyone, but will run under user’s own permissions. Information could potentially leak (spyware, tricking user to execute?)
prg2 not suid; executable by all but only writable by root
prg3 is a setuid program owned by root but not executed by any other (but permissions can be changed in the future so this can be dangerous).
prg4 setuid writable by anyone(!)
prg5 setuid and executable by anyone.

The absolute order depends partly on the student motivations. A common ranking, if motivations support it, can be prg4 > prg1 > prg5 > prg3 > prg2

(10p)

3 Cryptography (10 p)

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 AC (as opposed to SC, 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)

(exam continued on the next page)

4 Security Models (10 p)

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.

slides, example during lecture, or book Figure 13.6.

b) Define the simple security rule formally in the following way:
Simple Security Rule: A subject S can read object O only if ...

book page 457, or lecture on security models

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) Accepted Alice reads a document outlining which new offices will open in 2014 for Bank of Wales.
2) Denied Alice reads a document outlining which new offices will open in 2014 for Bank of England.
3) Accepted Alice reads a document outlining which new offices will open in 2014 for Air France.
4) Accepted Bob reads a document outlining which new offices will open in 2014 for Air France.
5) Denied Alice reads a document outlining which new offices will open in 2014 for Bank of England.
6) Accepted Bob reads a document outlining which new offices will open in 2014 for New York Times.
7) Accepted Alice reads a document outlining the yearly summary of earnings / losses for Bank of Wales.
8) Accepted Alice reads a document outlining the yearly summary of earnings / losses for Bank of Wales.
9) Accepted Bob reads a document outlining the yearly summary of earnings / losses for Bank of Wales.
10) Accepted Alice reads a document outlining the yearly summary of earnings / losses for Air France.
11) Accepted Bob reads a document outlining the yearly summary of earnings / losses for Air France.
12) Accepted Alice reads a document outlining which new offices will open in 2014 for Bank of Wales.

(10 p)

(exam continued on the next page)

5 Ethics (10 p)

There are two theories on ethics called the teleological theory and deontology. These may work either 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.

slides, example during lecture, offprint.

Let's look at the vulnerability reporting process. You have discovered a severe flaw in a home IoT system that is very popular. You realize that an attacker may use this flaw to listen to and record conversations in the home close to any of the devices.

c) Who would you tell about the flaw?
d) Who would you not tell about the flaw?

answer depends on reasoning and how theory is used

Make sure your answer contains 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. We expect you to at least list at least three parties in your answer in (c+d). (10 p)

6 Misc (10 p)

Give a short (i.e., less than ca. 5 lines) but exhaustive answer to each of the following questions. Answer in the following way.

A definition/explanation, followed by an example.

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 a polymorphic virus
b) What is a macro virus
c) Explain zero-day exploits
d) What are keyloggers
e) Explain spear-phishing
f) There are two fundamentally different ways of causing a denial of service attack. Describe them and give an example for each type.
g) What is meant by key escrow?
h) What is social engineering?
i) Explain the *side-channel attack*. Give an example.

a)-e) Malware Module, see pp208—209; p 216; 202/223—224
f) DoS Module: blackboard / slides
g) Cryptography module; slides + reading
h) section 6.4
j) slides;