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 29 August 2018, 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 Thursday 20 September 2018. 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 p ≤grade 3 < 38 p ≤grade 4 < 46 p ≤grade 5 (EDA263)

30 p ≤pass < 46 p ≤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.

(10 p)

2 Security and dependability concepts (8 p)

Briefly explain the following ways of categorising attacks. Give a brief example for each type.

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

(8p)

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 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?

(10p)

(exam continued on the next page)

4 Authentication (8 p)

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)

5 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.
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)

6 Ethics (5 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.

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/
d) 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. (5 p)

7 Misc (9 p)

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) Biometric authentication systems are becoming more prevalent (e.g., fingerprint sensors on phone). Explain why there might still be false matches in such systems even though fingerprints are believed to be unique. Are there any other sources of problems? (3p)
b) Explain briefly how *speculative execution* was used in the Spectre attack. What side-channel attack was used in this attack and how? (3p)
c) Some exploits, such as Rowhammer, means that you may be able to deterministically shift a single bit on a system. How can a single bit-shift have security implications? Give an example on how the attacker would use such an attack. (3p)