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 23 March 2019, 08:30—12:30

Examiner: Associate professor Magnus Almgren, Ph.031-772 1702,
email: magnus.almgren@chalmers.se

Teacher available during exam: Magnus Almgren, Ph.031-772 1702
The teacher will aim to physically come twice to the exam: about 60—90 minutes after the start of the exam, and about 60--90 minutes before the end.

Language: Answers and solutions must be given in English.

Grades: will be posted before Monday 15 April 2019. The exam review date/place will be announced on canvas 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 $\leq$ grade 3 < 38 p $\leq$ grade 4 < 46 p $\leq$ grade 5 (EDA263)

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

1 Introduction and Terminology (14p)

One of the challenges of computer security is potential attacks on the security mechanisms. Describe your own scenario of how a security mechanism (or a change therein) can be turned into an attack by answering the following questions.

a) As part of your answer: define the following terms and use them in your example: *threat, vulnerability, countermeasure.* (6p)

The terms are described in Table 1.1 page 38. How they are used with your example depends on your scenario and you should use these for answers in (b—d).

*(b-d) is concerned with the discussion of challenges on p36, esp. point 2. What we are looking for is not a new more advanced attack that existed before / after (c). The idea is rather how a *new* attack is introduced with the security mechanism.*

Any system that takes a known action as a response to some input could run the risk of being used by the attacker.

b) Describe the initial setup (before introducing the security mechanism) (4p)

c) Explain how a security mechanism (or change therein) can mitigate the attack from (b). The security mechanism should be known and discussed in the course book. (2p)

d) Explain how the attacker can use the security mechanism proposed in (c) to create a new type of attack. (2p)

2 Malware (6p)

a) What is speculative execution? (2p)

b) How was speculative execution used in the Spectre attack.
Give a brief example supported by some pseudo code. (2p)

c) What side-channel attack was used in this attack and how? (2p)

See slides in module "Malware and Attacks", esp. L07 C recent-malware-2018.pdf

3 Intrusion Detection Systems (10p)

a) Explain the principles of anomaly-based intrusion detection. (2p)

b) Explain the base-rate fallacy by giving a numerical example.

The IDS you use analyzes potential malware in email attachments and is about 95% accurate.

In the beginning of your answer, you should choose (and state) the number of units analyzed per day, and how many of these are malicious.

Then use these numbers to give a numerical example to explain the base-rate fallacy. Show the steps in your calculations, and approximate as necessary. (8p)

See slides in module "Intrusion Detection", esp. L12 intrusion detection systems

(exam continued on the next page)

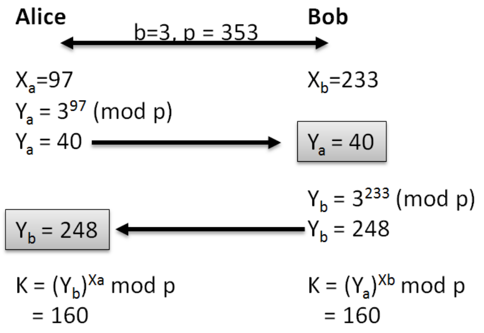
4 Cryptography (6p)

You are sitting on an airplane when you notice that the passenger next to you is correcting exams. You glance over and see the following (partial) answer from one student. You realize this is the Diffie-Hellman algorithm discussed in the lectures.

a) What is this particular algorithm mainly used for? (2p)

b) What is the underlying security assumption? (why is it considered secure?) (2p)

c) What happens if the information (marked with arrows) is sent in clear text (not protected by encryption) and the adversary Eve manages to sniff the network and extract these parameters? (2p)



See slides in module "Cryptography", esp. L02 Cryptography.pdf. One-way functions and trapo-door one-way functions are discussed, and where the Diffie-Hellman is shown and p83.

5 Security Models (8p)

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 in module "Security Policies and Models", esp. L14 Security Plicies and Models.pdf

6 Authentication and Access Control (16p)

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 misclassifications even though fingerprints are believed to be unique. (4p)

b) Many times a *slow hash function* is used when authenticating users with passwords. Why is a hash function used? Why is it slow? Explain two (2) reasons why a *salt* is used in combination with the password. (4p)

c) What is the difference between a password and a passphrase? What is the preferred method for modern authentication according to NIST guidelines? Why? (4p)

d) Describe the reference monitor and what it is for? Draw a figure demonstrating its function and the in/out data necessary. (4p)

a) Book page 112; Features; context of collection with noise, figure 3.7
b) Book page 97
c) See direct download: Guidelines to choose a good password from NIST
d) See slides: Module "Operating System Security" as well as book page 460.