Mittuniversitetet
MID SWEDEN UNIVERSITY

Försättsblad Prov Original

Kurskod	Provkod	Tentamensdatum
DT145G	T104	2019-01-09

Kursnamn	Datateknik GR (B), Datorsäkerhet
Provnamn	Tentamen
Ort	Sundsvall
Termin	
Ämne	

6895642268

Utskriven 2019-02-21 kl. 07:39:32

Mittuniversitetet
MID SWEDEN UNIVERSITY

Final exam

DT145G Computer Security

Daniel Bosk

Department of Information Systems and Technology,
Mid Sweden University, SE-851 70 Sundsvall
Email: daniel.bosk@miun.se
Phone: 010-142 8709

2019-01-09

Instructions

Carefully read the questions before you start answering them. Note the time limit of the exam and plan your answers accordingly. Only answer the question, do not write about subjects remotely related to the question.

Write your answers on separate sheets, not on the exam paper. Only write on one side of the sheets. Start each question on a new sheet. Do not forget to *motivate your answers*.

Make sure you write your answers clearly, if I cannot read an answer the answer will be awarded no points—even if the answer is correct. The questions are *not* sorted by difficulty.

Time 5 hours.

Aids Dictionary.

Questions 9

Preliminary grades

Each question can be awarded up to three points: one point for E, two points for C and three points for A. To get an E, you must get at least one point on each question — i.e. no question must be awarded zero points. For a C, you must get two points on at least half of the questions. For an A, you must get three points on at least half of the questions.

Questions

The questions are given below. They are not given in any particular order.

1. Describe the terms

(2p) (a) identification and

(2p) (b) authentication.

Make sure to illustrate your explanations by examples. You must also give an example of a mechanism for each of the terms.

2. Separation of duties is a core concept for security.

(2p) (a) Describe the two types of separation of duties.

(1p) (b) What is the main reason for separation of duties?

(3p) 3. Give an example of a passive side-channel attack.

(3p) 4. There are three approaches to security: prevention, detection and reaction. Discuss why security is not all about prevention, how do the three approaches complement each other.

(3p) 5. Discuss why usability is important for security.

(3p) 6. A user wishes to provide confidentiality to a file.

(a) She can accomplish this through mechanisms provided in the operating system. Explain how this works and what are the limits.

(b) She can also accomplish this through purely cryptographic mechanisms. Explain how this works and what are the limits.

(3p) 7. Can a files such as images (e.g. JPEGs) and other data be dangerous?

(2p) 8. What is mandatory access control?

9. You are asked to estimate some password policies. The policies are the following:

basic12 At least 12 characters consisting of upper and lower case, and numbers.

randswedict4 Randomly choose four words from the Dictionary of the Swedish Language (SAOL). This dictionary contains approximately 125 000 words.

You should answer the following:

(4p) (a) Estimate the entropy for the passsword policies. (You may rely on the results in certain published research papers discussed in the course for certain estimates.)

(2p) (b) Decide how suitable they are for use in a large organization.

(2p) (c) Decide how suitable they are for use in a web application.

Note that you will not get any points without a motivation.