Mittuniversitetet
MID SWEDEN UNIVERSITY

Försättsblad Prov Original

Kurskod	Provkod	Tentamensdatum
DV026G	T104	2018-06-07

Kursnamn	Datavetenskap GR (B), Informationssäkerhet
Provnamn	Tentamen
Ort	Sundsvall
Termin	V18
Ämne	Datavetenskap

Mittuniversitetet
MID SWEDEN UNIVERSITY

Final exam

DV026G Information Security

Daniel Bosk

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

2018-06-07

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, course material and notes, calculator.

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.

(3p) 1. You've just landed a job at an IT department somewhere and now you're having one of your first few days. There is a discussion in the "fika room", the topic is the IT department's password policy.

"Well, every respectable website requires at least eight characters, with lower and upper case, numbers and special characters", the head of department says, "so we have it too".

What would you like to say in this conversation?

(3p) 2. What is the purpose of separation of duty? Explain and illustrate your explanation with an example.

(3p) 3. Describe the terms identification and authentication as well as how these relate to each other. Make sure to illustrate your explanations by examples.

(3p) 4. What is mandatory access control? Discuss its advantages and disadvantages and its suitability in different situations.

(3p) 5. Analyse and compare the three malware reproduction techniques virus, worm, trojan horse.

(3p) 6. There are numerous alternatives available today for end-to-end secure communication[1], e.g. the apps Signal, WhatsApp and Telegram for instant messaging, media messaging and video calls; PGP and S/MIME for email. They are all based on a combination of public-key and shared-key cryptography.

Discuss the usability challenges facing end-to-end secure communication.

(3p) 7. 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) 8. Given an example of an active side-channel attack.

(3p) 9. Alice wants to provide confidentiality to a file.

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

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

[1] Normally this is referred to as end-to-end *encrypted* communication, but we have integrity in addition to confidentiality.