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

2015-10-30

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.

Maximum points 39

Questions 6

Preliminary grades

The following grading criteria applies: E $\geq$ 50%, D $\geq$ 60%, C $\geq$ 70%, B $\geq$ 80%, A $\geq$ 90%. No question must be awarded zero points.

Questions

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

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

   comprehensive8 At least 8 characters consisting of upper and lower case, numbers and special characters (assume the ones common with the numbers on a keyboard).

   randswedict3 Randomly choose three 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 the home environment.

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

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

2. 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.

3. Multi-level security and multi-lateral security are two related terms.

(3p) (a) Explain what multi-level security is and what we want to accomplish with it.

(3p) (b) Explain what multi-lateral security is and what we want to accomplish with it.

(3p) (c) Give some of the advantages of combining them and explain why this is so.

4. Define the following terms:

(1p) (a) Trusted

(1p) (b) Trustworthy

(1p) (c) Secrecy

(1p) (d) Confidentiality

(1p) (e) Privacy

(1p) (f) Integrity

(1p) (g) Authenticity

(5p) 5. Your boss is finally convinced that the company needs an Information Security Management System (ISMS, Swe. 'ledningssystem för informationssäkerhet'). He comes to ask you how an ISMS is best implemented, explain how that is done.

6. Human psychology is important in security. It is used in both security usability and social engineering.

(2p) (a) Give an overview of why psychology is important in security.

(4p) (b) Give an example of an attack which exploits weaknesses in human psychology. Also explain why it works.

References

[And08] Ross J. Anderson. *Security Engineering. A guide to building dependable distributed systems.* 2nd ed. Indianapolis, IN: Wiley, 2008. ISBN: 978-0-470-06852-6 (hbk.) URL: `http://www.cl.cam.ac.uk/~rja14/book.html`.