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

2016-08-16

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 26

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.

(3p) 1. Describe the requirements for a process to be able to assess the integrity of itself and its execution environment.

> **Suggested solution** If the process can trust its environment (i.e. the operating system), then it can rely on the environment to assess its own integrity. Thus the process relies on the integrity of the operating system. The oerating system in turn relies on the integrity of the hardware and must rely on the hardware to assess its own integrity. Hence the process needs hardware that will not allow a modified version of the operating system to run.

2. Explain the following terms:

(1p) (a) Confidentiality

(1p) (b) Integrity

(1p) (c) Availability

(1p) (d) Accountability

(1p) (e) Non-Repudiation

> **Suggested solution** See [**Gollmann2011cs**] and [**Anderson2008sea**] for definitions.

3. Describe the three malware reproduction techniques

(1p) (a) virus,

> **Suggested solution** The virus inserts its own code into other programs code. When the other programs are run the virus' payload is run too and the infection can spread further.

(1p) (b) worm,

> **Suggested solution** The worm spreads by its own means, e.g. by utilizing networks (shared file systems, remote executions bugs in network services) or emailing itself using available programs on the computer.

(1p) (c) trojan horse.

> **Suggested solution** The trojan horse is a legitimate-looking program which contains unwanted functionality. E.g. it is a flash-light app, but in the background it uploads the contact list to the app's developer.

4. Explain how information theory can be used to estimate the strength of passwords chosen under a given password composition policy:

(2p) (a) How can you estimate the upper bound, i.e. the maximum possible entropy?

(2p) (b) Why can't you estimate any (useful) lower bound, i.e. the minimum possible entropy?

(2p) (c) How can you estimate the average case, i.e. what is usually the case when users choose the passwords?

Suggested solution You assume that every part of the password is chosen uniformly randomly. This gives the maximum entropy, i.e. it is an upper bound. You have to account for all choices the password composition policy allows. Or rather, all choices the policy removes.

This is hard because a user can choose a very easy to guess password, which has almost no entropy. Similarly, if all users choose the same password, then the entropy would be zero.

The average case can be estimated as in [**Komanduri2011opa**]. You have to *sample a lot of user-generated passwords*, then you can perform a frequency analysis to find the probabilities and compute the entropy. The users are the stochastic variable (random output) and you must get a large enough sample to estimate the probability distribution.

(4p) 5. Describe a scenario where a covert channel is used.

Suggested solution A server is anonymous (e.g. a Tor hidden service), i.e. you may access the server but not know its location. Part of the server's service is giving the time. It has been shown that the variations in the system clock depend on the ambient temperature. This means that by studying how the time on the server varies over day and night and over the seasons, we can eventually figure out the ambient temperature. From the ambient temperature we can later deduce the geographical location of the server.

6. Explain the following terms:

(1p) (a) Brute force

(1p) (b) Dictionary attack

(1p) (c) Social engineering

(1p) (d) Two-factor authentication

(1p) (e) Phishing