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

2015-06-01

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 28

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. Explain the following terms:

(1p) (a) Confidentiality

(1p) (b) Integrity

(1p) (c) Availability

(1p) (d) Accountability

(1p) (e) Non-Repudiation

> **Suggested solution** See [Gol11] and [And08] for definitions.

2. A user wishes to provide confidentiality to a file.

(3p) (a) She can accomplish this through mechanisms provided in the operating system. Explain how this works and what are the limits.

(3p) (b) She can also accomplish this through purely cryptographic mechanisms. Explain how this works and what are the limits.

> **Suggested solution** The first way she's securing her file is by using access control mechanisms in the operating system (OS).
>
> Assuming we have physical access to the computer, then we can just read the raw data from the disk. This can be accomplished by either booting our own OS on her computer, or by removing the disk.
>
> If we don't have physical access we can always try to bypass the access control mechanisms in other ways, e.g. by gaining privileges in the system or seeing if the OS has failed to protect reading from the raw disk (i.e. not using the file system).
>
> The main point here is that the operating system must be working correctly for its mechanisms to be effective. The *running* operating system will provide confidentiality by not allowing other users' requests to open the file.
>
> The most obvious way to have system independent security for this file is to encrypt it, i.e. using cryptographic mechanisms. This way no one can read it unless they have access to the key, and this is true no matter if you change the environment. (Of course, if the system is untrusted someone can get to the key that way, but that's outside the scope of this question.)

3. 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 [Kom+11]. 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.

4. 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.

Suggested solution In identification you claim an identity. This can be done using e.g. a username, fingerprint or DNA sequence.

In authentication you prove you are who you claim you are. This can be done using e.g. *who* you are (biometric), *where* you are (location) or what you *do* (biometric), something you *have* (e.g. BankID), or something you *know* (password).

(4p) 5. Describe the main differences between Mandatory Access Control (MAC) and Discretionary Access Control (DAC).

Suggested solution In MAC the access control policy for new material is derived from the subject and objects it is based on. One example is Bell–LaPadula (BLP): where information only flows upward, a document produced by someone with clearance A will also require clearance A to be read—clearance $B < A$ will not suffice. The system sets the access policy for objects.

In DAC this is under the control of the owner of an object. The owner sets the access policy. An example is the UNIX file system.

6. 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?

Suggested solution There are two types of separation of duties: dual control and functional separation. Dual control means that two or more subjects must act together (at the same time) to authorize a transaction. Functional separation means that several functions are needed to authorize a transaction—e.g. create a transaction and verify it—and one subject is not allowed to do both functions.

The reason for separation of duties to make it impossible for one malicious subject to compromise a system. With separation of duties the malicious subject must persuade one or more other subjects to collude.

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`.

[Gol11] Dieter Gollmann. *Computer Security.* 3rd ed. Chichester, West Sussex, U.K.: Wiley, 2011. ISBN: 9780470741153 (pbk.)

[Kom+11] Saranga Komanduri, Richard Shay, Patrick Gage Kelley, Michelle L. Mazurek, Lujo Bauer, Christin Nicolas, Lorrie Faith Cranor, and Serge Egelman. "Of passwords and people: Measuring the effect of password-composition policies". In: *CHI*. 2011. URL: http://cups.cs.cmu.edu/rshay/pubs/passwords_and_people2011.pdf.