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

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, 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. Describe the terms

   (a) identification and

   (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).

(3p) 2. Separation of duties is a core concept for security.

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

   (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.

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

> **Suggested solution** The adversary is interested in learning classified information. They set up a device which records electromagnetic emissions to reconstruct the image on a screen, thus when a target works with the classified data on the computer the adversary sees the same image. This is a passive attack since we only need to record.

(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.

> **Suggested solution** The reason for having these three approaches is partly economy and partly that it is impossible to do prevention for certain things. Thus, if we cannot prevent an attack, we must be able to detect it. When we have detected it we must be able to recover.
>
> In some cases it's impossible to recover, however. For instance, if the attacker gets the personal data of clients. We simply cannot take back this data, there will always be a copy somewhere. Thus prevention is the main approach for protecting personal data. Prevention in this case comes both in terms of protecting the stored data, but also through data minimization, i.e. storing only the necessary data, nothing more.

In other cases, the recovery might be in terms of insurance paying for the costs of the damage, e.g. financial loss.

In some cases, prevention is possible, but detection and recovery is cheaper. For instance, the lunch coupons for restaurants can easily be frauded. But this will also be easily detectable, thus the cost of prevention might be higher than the cost of the fraud before detection.

In other cases, e.g. electronic communication, then prevention is cheap — simply use encryption — whereas detecting a passive eavesdropper is impossible.

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

Suggested solution Då systemen vi är beroende av och som ska upprätthålla vår säkerhet handhas av människor blir psykologin genast viktig. Vi behöver psykologin inom säkerhetsområdet för att kunna ta hänsyn till hur människor fungerar när vi konstruerar säkerhetssystem. Exempelvis, om vi gör ett system för komplext och användaren tycker att komplexiteten är onödig, då kommer denne användare att aktivt försöka att ta sig runt systemet — kanske genom att skriva upp långa lösenord istället för att lära sig dem utantill.

Om vi däremot tar hänsyn till användarnas kognitiva begränsningar, då kan vi konstruera system som både är säkra och enkla att använda.

(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.

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.)

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

Suggested solution Yes, they can contain machine code which can be executed if there is e.g. a buffer overrun vulnerability in the software that reads the data.

(3p) 8. What is mandatory access control?

Suggested solution Mandatory access control sets the access policy for created objects based on fixed rules in the system.

(3p) 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:

(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.)

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

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

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