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

2017-05-26

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 27

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. (a) Give an example of a covert channel and

> **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.

(b) what we can do about it.

> **Suggested solution** We can lower the resolution in the time-stamps the server gives, e.g. by not giving seconds. This lowers the bandwidth of the covert channel, perhaps so that the attack is infeasible. We could also sync the servers clock more often, e.g. by using the Network Time Protocol. However, the only way to prevent it is by not revealing the time of the server's system clock.

(3p) 2. The terms "data" and "information" are related but not the same. Discuss how they are related and how this affects the term "security", as in "data security" and "information security".

> **Suggested solution** Data is an encoded representation of information. Data can be manipulated by formal rules to infer new information. E.g. the data "$x+1=0$" does not directly reveal the value of x, but we can manipulate the data with formal rules (equation solving) and infer the value of x ($x=-1$).
>
> The same applies for other situations: When sending data over an anonymizing network (e.g. Tor), we only reveal the size and timing of the packets sent. However, these can be statistically correlated to the packets exiting the network, thus the sender and recipient can be inferred.

(3p) 3. (a) What is discretionary access control?

(b) Discuss some of its advantages and disadvantages.

> **Suggested solution** The owner (creator) of the object may set the access policy for the data object. This is what is common in normal file systems and systems like Facebook.
>
> This puts more responsibility on the user than mandatory access control would: it's the responsibility of the user to analyse and prevent information leaks. From a usability perspective, it's of course possible to add a layer on top which does this analysis and presents it to the user.

(3p) 4. 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.

5. 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.

(3p) 6. 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.

> **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. You work for a start-up company which offers low-cost flat-rate subscriptions for live streaming. This will require authentication.

(a) Analyse what data must be authenticated on registration (i.e. the set-up of a new subscription). Suggest how to do the authentication.

> **Suggested solution** That the user doing the registration is the user owning the payment data. This is usually stipulated by the payment service, e.g. Visa or MasterCard: card number as identifier and CVV code as "password".

(b) Analyse what data must be authenticated during streaming. Suggest how to do the authentication.

Suggested solution First, we must to know that the user has a paid subscription. Second, we might also need to enforce some age requirements. We can use anonymous credentials to reveal as little information as possible.

(3p) 8. The systems administrator has (due to their role) unlimited access to all computer systems in the organization — they set up and configure all systems. How can you ensure accountability for the systems administrator?

Suggested solution This can be solved with separation of duties. The systems must log to a system that the systems administrator cannot access. Thus the systems administrator can be held accountable for what he does.

Of course, we cannot trust the systems administrator to set this up himself, so we need functional separation.

(3p) 9. Shannon entropy can be used to estimate how well the users choose passwords under a given password composition policy:

(a) How can you estimate the upper bound, i.e. the maximum possible entropy? And what does the upper bound mean?

(b) Why can't you estimate any (useful) lower bound, i.e. the minimum possible entropy? What would a lower bound mean?

(c) How can you estimate the actual entropy of 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. This means that users cannot do any better than this. You have to account for all choices the password composition policy allows. Or rather, all choices the policy removes.

A lower bound would provide a guarantee that users choose passwords sufficiently randomly. This is hard because a user can choose a very easy to guess password for any static password policy, which has almost no entropy. Similarly, if all users choose the same password, then the entropy would be zero. This is why a lower bound is not very useful, it will 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.