Mittuniversitetet
MID SWEDEN UNIVERSITY

Final exam

DT145G Computer Security

Daniel Bosk

Department of Information Systems and Technology,
Mid Sweden University, SE-851 70 Sundsvall
Email: daniel.bosk@miun.se
Phone: 010-142 8709

2018-06-07

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.

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. You've just landed a job at an IT department somewhere and now you're having one of your first few days. There is a discussion in the "fika room", the topic is the IT department's password policy.

"Well, every respectable website requires at least eight characters, with lower and upper case, numbers and special characters", the head of department says, "so we have it too".

What would you like to say in this conversation?

> **Suggested solution** The last decades' research in user authentication says that such a policy yields bad security. It forces users to select easy to guess passwords and incentivizes password reuse while more secure passwords are disqualified according to the policy.
>
> A better policy is to have at least 12 characters as the only requirement. Also, no requirement of updating the password at regular intervals — only if a breach has occurred.

(3p) 2. What is the purpose of separation of duty? Explain and illustrate your explanation with an example.

> **Suggested solution** The purpose of separation of duty is to make it more difficult for a malicious entity to subvert the system. E.g. a systems developer at the bank should not be able to add a back-door for himself so that he later can steal money without anyone noticing. If he is only allowed to write the code, but not to certify its correct function — then there is a higher chance that he is caught before the system is launched. So to subvert the system a malicious actor must act together with others.

(3p) 3. Describe the terms identification and authentication as well as how these relate to each other. Make sure to illustrate your explanations by examples.

> **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 the validity of a claim. E.g. in the case of identification, prove that you are who you claim you are. This can be done using e.g. *who* you are (biometric), what you *do* (biometric), something you *have* (e.g. BankID), or something you *know* (password).
>
> Authentication can also be applied to other attributes than identity, e.g. that you are older than a given age limit. This can be proven without revealing your identity or birthday.

(3p) 4. What is mandatory access control? Discuss its advantages and disadvantages and its suitability in different situations.

> **Suggested solution** Mandatory access control sets the access policy for created objects based on fixed rules in the system. Two examples are the Bell-LaPadula and Biba models. BLP prevents information flow that can violate confidentiality and Biba prevents information flow that can violate integrity.
>
> Mandatory access control helps enforcing the policy and to avoid mistakes. On the other hand, it will prevent communication downwards (or upwards), which might be necessary sometimes (this is usaully solved by special procedures for declassification).
>
> However, whether it is good or bad depends on the situation. Sometimes it's good to have a combination of mandatory and discretionary access control.

(3p) 5. Analyse and compare the three malware reproduction techniques virus, worm, trojan horse.

> **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. It requires that programs move between systems to spread from one system to another, e.g. by USB-drive or network drives. Nowadays, when manual file copying of program executables have decreased, viruses are not good for spreading across systems.
>
> The worm, on the other hand, 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. This is a much better proliferation technique.
>
> 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. The advantage of this class is that the malware will not be suspected, the desired program is running etc., no new processes as for worms.

(3p) 6. There are numerous alternatives available today for end-to-end secure communication[1], e.g. the apps Signal, WhatsApp and Telegram for instant messaging, media messaging and video calls; PGP and S/MIME for email. They are all based on a combination of public-key and shared-key cryptography.

Discuss the usability challenges facing end-to-end secure communication.

> **Suggested solution** The challenge for these systems is to provide a design which aligns the security with how users work.
>
> The easy part is to provide a tool for securing the communication, i.e. encrypting and providing integrity checks.
>
> The hard part is to do proper key management, specifically to authenticate the owners of the other keys. The currently most used approach is that of Signal, WhatsApp and Telegram. They authenticate phone numbers by sending text messages to the phone number. Thus they can be sure that the owner of the phone number is also the owner of the private key. (Well, the phone operator can of course impersonate the owner of the phone number.) Then another user has identified another user by his or her phone number, then the app will ensure the verified key is used.

(3p) 7. 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.

[1] Normally this is referred to as end-to-end *encrypted* communication, but we have integrity in addition to confidentiality.

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

(3p) 8. Given an example of an active side-channel attack.

Suggested solution Extracting the secret key from a device by measuring energy consumption or electromagnetic emissions while the device performs computations using the secret key. It is an active attack since we might need the device to perform operations on certain ciphertexts (or plaintexts).

(3p) 9. 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.)