Rolf Vidar Hoksaas — rolfvh
Institutt for Informatikk
Universitetet i Oslo

October 1, 2019

OBLIGER 1 — Applied security

1 Preamble

“A high school are going to start using a new digital platform for learning (LMS, Learning management system). The learning platform will run on servers stored in aserverroom in the school, where all the data in the system also are being stored. The computer system will be available through the internet as both a web application (web page) and a mobile application. Data (information) which are being stored and processed in the system includes:

- *Information about the pupils: Full name, class, name of parents, adress, cell phone numer, date ofbirth.*
- *Information about the teachers: Full name, classes, address, cell phone number.*
- *Digital assignments from the pupils: The pupils submit digital school work (e.g. documents, recordings of audio or video) in this system.*
- *Teacher feedback on the submissions, including grades.*
- *Interim evaluation and overall achievement grades.*

Your task is to make an overall evaluation of various information security issues, which the school-management must then consider and possibly deal with before the computer system can be used. All tasks should be solved based on the scenario given above.”

2 Questions

“Identify a couple of values in this scenario. Can you imagine values that are more important to a student than a teacher, and vice versa? Explain briefly, with examples. Also, name a couple of likely threat actors.”

Values in this scenario include the privacy of the teachers and pupils: their personal information must remain hidden unless required. For a student it is also important that grades are kept confidential, while a teacher cares about solutions not being given to the students before a test. Threat actors regarding these values could be external actors or students wishing to change their grades, or students wanting to get ahold of answers to tests.

This assumes teachers store solutions on the server. □

“*CIT-services (confidentiality, integrity and accessibility) are essential features of information security. For each of them, consider the importance as well as things that may go wrong. That is, what may represent a threat or danger to each security objective.*”

Confidentiality is an important aspect of a LMS. I consider this to be the most important, both for students and for teachers, in comparison to the other elements of the triangle of security. The information of any user must be kept private, in order to respect their privacy. Having said that, integrity and accesibility are not neglectable.

Integrity of submissions is relevant, as quality of grading depends on this (while authenticity, especially of author, is vital in order to give the correct score to the correct person).

Accessibility and availability is, from my point of view, the least important aspect of security, although not irrelevant. Not having access to your grades or your students' submissions your account can lead to issues such as due times on registrations, for instance, but these are more easily fixed in hindsight. Fixing leaks is usually not as easy. □

“*Give two general security controls that in this case can help to achieve*

a) Confidentiality

b) Integrity

”

There is a really straightforward solution for confidentiality, but it is not always as simple to execute: Follow the mandatory rules given by GDPR. This includes not saving more information than necessary, always saving data with encryption, never in rawtext, and having access control over all critical points of information. Having a good control over this is vital, but requires people to not share their access information such as their password or tokens to anyone.

Having a strong access control system is also relevant for integrity for two main reasons. As mentioned above, authenticity is of great relevance to submissions, but so is also maintaining the integrity once stored on the servers. By having redundant copies of the same data, many problems regarding integrity can be solved, as there will most likely be a backup or duplicate somewhere which remains unaltered even after a security breach. □

“*Explain the role of accountability and authentication. Would you recommend prioritizing these security goals (security services/properties) in our case? Justify your answer.*”

Regarding accountability, in the case of a problem rising, I think it's to a certain degree relevant to be able to blame someone, but I find it more important to come up with solutions, and remove the possibility for it to happen again. So, no, I wouldn't prioritise accountability over other topics. Nevertheless, having someone responsible for the security of the system is important. They are implicitly accountable for the risks and consequences, and are the ones that would know the system.

The need for authentication has somewhat been explained earlier, although not in detail. Having restricted access to different things through access control allows the system to limit what is available to each user. This allows different permissions to be given to different users.

A teacher will be able to change and view the grades of all their students, but also view and give feedback on submissions, while a student will only be able to view their own grades, and submit deliveries to the system. □

> *“The school Skolen has an overall authorization policy which includes the following:*
>
> — *Pupils shall have access to view/read personal information about themselves, and only themselves.*
> — *Teachers shall have access to read/view personal information about all pupils they teach in atleast one subject.*
> — *Employees in the school administration shall have access to both view/read and change all personal information about both teachers and pupils.*
>
> *This policy applies regardless of how the information is requested, e.g. orally to the administration at the school, or directly in one of the computer systems the school uses to store and process this type of personal information.*
>
> *This means that the new digital learning environment must also enforce these policies. Briefly explain the overall mechanisms/functions that must be in place in the computer system for this to be implemented.”*

To set up a system where different users have different permissions, one would preferably set up a system with mainly four groups —sysadmin, administrative, teacher, pupil—, but also different groups for each teacher, assigned to the pupils they lead; where each group defines read and write properties of each other member, depending on what groups they pertain to.

All users must be given a unique password, and allow them to change it if they so desire.

Setting up the software to afterwards alter or view the details of each member should be straightforward as long as the software runs the commands as the user.

Logging all events is also a smart option, in order to check prior information, or recovering in case of malicious actions happening. □

> *“The school management also consider using a module in the system where pupils or their parents can report absence and the reason for absence, and where teachers can register a pupil’s absence. Does the school have to pay special attention before they can use this module? Justify your answer.”*

Since parents’ don’t have accounts of their own at the school, a parent should be enforced to send the notice through the same phone number which is registered to the pupil. Otherwise, there would be no confirmation regarding the truthness of what is said since there is no confirmation of who said it. □

> *“Student Network: The school’s wireless network (WiFi) har been set up without a “password” for encryption. Why is this a bad idea? Does turning on “encryption” in the wireless network affect whether it is safe to allow students and teachers to share a wireless network? Explain*

”

briefly.

If there is no password on the network, there is no control over who has access to network, which can lead to unwanted monitoring of the network traffic, and unwarranted consumption of the bandwidth. This facilitates malicious usage of the line, which is not desired.

Furthermore, if the data going over the network is not encrypted, third-parties can monitor all transactions going over the network, both bounded internally and those going to the internet, which is a severe security issue. They would be able to read passwords, compromising the entire system, and putting the data at risk. □

> “*Think like a “hacker”: As a student, you will try to change a grade in the system.* ”

Give an example of how you would do this! (PS. No exact answer :-))

If I needed to get my grade changed in the system, I would probably infiltrate as a serviceguy fixing the lights in the office of the teacher who has control over my grade.

Few people would make any questions to this, and would probably consider it routine. Waiting for them to go to the bathroom, I would get access to their computer, possibly with a keylogger if they have locked their computer, and if they haven't, I would directly access the files storing my password. Otherwise, I'd have to return after they have logged in at least once. □

Submitted by Rolf Vidar Hoksaas — rolfvh on October 1, 2019.