Secure software development and web security
Computer project

R. Absil

January 2026

This document details the features required for the computer project to implement for the security course. You will find here details about the requirements of your applications, along with the constraints to respect and the submission procedure. Deadlines are given in Section 4.

Contents

1 Introduction

The goal of this project is to implement a *secure* client / server system handling medical records.

A lot of freedom is left to your discretion regarding the security policy and actual data storage. Considering the main aspect of this project is security, appropriate techniques have to be used, whether they have been covered in class or not.

Hence, although you are free to choose protocols and languages that you find appropriate, you are responsible for these choices. That is, should you favour some technique over another, and if it figures the choice you made is not relevant regarding security, you will be penalised.

Moreover, between to equivalently secure solutions, you have to favour the most efficient one, even if it complexifies the system.

Finally, the features labelled "Master note" and ended by the "◀" symbol only apply to students in a Master's cursus.

2 System Characteristics

The architecture to use for your system is "client / server". Consequently, there are only two types of actors: a server, and a set of clients driven by users.

From a general point of view, the server allows:

- new users to register to the system;
- users to log in the system;
- authenticated users to perform various tasks, when the context is appropriate.

Information described in the next part of the document specifying these features is deliberately high-level: it is your job to detect the key points to secure in your project, and how to do it. For that purpose, you are allowed to deviate from what is written here in order to strengthen security.

The server

The server is a *not* trusted entity. In particular, you do not know its set of public keys. Consequently, you have to provide a mechanism to "securely" transfer it and checking its ownership.

Furthermore, the server should not be trusted with *any* kind of sensitive information, such as confidential data, sensitive authentication and cryptographic material. Hence, you are expected to decide what security to implement regarding the transmission of data to the server, as well as regarding the storage of data on the server.

Furthermore, note that in no way you may consider that the server is uncompromised regarding storage. That is, if the server is compromised[1], the confidentiality of any sensitive information stored to the server must never be put in jeopardy.

Master note: Note that, for each "pack of data" or request sent to the server, an associated set of metadata is also sent to the server. This metadata contain at least

- the time the actual data or request was sent,

[1] For instance, if an administrator maliciously updates the server so that he recovers every password sent to it, or steals any cryptographic key stored on the server.

- the size of the data or request,
- the privileges needed for the request (if relevant),
- the tree depth of the required resource (if relevant),

and any other metadata you see fit meant to be used by the server for anomaly detection purposes[2]. Note that this metadata cannot in any way depend on the content of actual data or request, which is highly sensitive.

◀

Users

There are two types of users:

- doctors,
- patients.

Doctors are said to be *trusted* users.

For simplicity reasons, any user can be of one type only (so, there is no doctor-patient). The rights that these users have are described in Section 3.

Patients have the following attributes:

- first and last name,
- date of birth,
- a medical record,

and a list of associated doctors (the specialists that actually take care of them). We say that these doctors have been *appointed* to the patient. Obviously, a doctor can be appointed to multiple patients.

Doctors have the following attributes:

- first and last name,
- medical organisation (such as an hospital).

For simplicity reasons, doctors belong to a single medical organisation.

[2] A machine learning model is not expected here, since you won't have enough data to train it.

Medical records

By medical record, we mean a directory containing various files[3] each with an associated date (the date of the examination / appointment). Note that the content of the files, their names and dates are considered sensitive information.

3 Features

In each of the following protocols, data exchange must be secured at best (according to the relevance of the implemented protection). The same remark can be applied to the storage of data resulting from an exchange. Obviously, if some files are stored ciphered, when a user downloads them, the system has to decipher the considered files.

The type and level of security to use are left to your discretion. Consequently, it is recommended to implement more measures than those dedicated to integrity, confidentiality and authenticity, such as denial of service, dictionary attacks and injections.

Master note: It is expected that a robust system of logs records user's activity, and that there is sufficient monitoring against attacks, for instance with a form of input sanitisation and automated log analysis. It is also *mandatory* that separation of duties is enforced by the architecture of your logs. ◀

Again, note that you are allowed to deviate from the protocols described here, as long as these changes are motivated by security. However, you are responsible for these choices: should you change a protocol by another less secured, you will be penalised. Additionally, out of two equivalently secure solutions to a problem, you have to favour the most efficient one[4].

Finally, remember that *only* security is graded here: you won't be penalised if you decide not to follow the guidelines and good practices of web-development (as long as it has no negative impact on security and efficiency).

User registration, authentication and revocation

When a new user wants to register to the server, after the authenticity of the server has been verified, credentials have to be generated for the user. The form of these credentials (passwords, keys, etc.) is left to your discretion. Remember that the server is not to be trusted with the any kind of sensitive information, in particular, sensitive authentication material.

After this step, the user can log in the system with its credentials.

Note here that we make an amalgam between users (people) and clients (devices). You can choose to authenticate users and/or devices.

[3] For simplicity reasons, no particular structure has to be enforced in medical records.

[4] Obviously, simplicity is to be favoured over complexity, but if a simpler solution hinders the performances of a system, you have to complexify your application to make it more efficient.

Master note: Any user can, at any point, change his credentials and any piece of information he uses to securely communicate with the server, or store information. Furthermore, it must be possible for users to log in from different devices. ◀

Master note: Considering the additional attributes of trusted users, it is expected that some form of integrity, accountability and non repudiation is provided regarding these attributes.

We strongly suggest that trusted users own a certificate signed by a CA that the server trusts. Since CA-signed certificates are assumed to be handled in a "decentralised" way, you will have to setup a PKI *and* a chain of trust (at least with three nodes) for the server to actually check the validity of certificates. In *no way* can you consider that your backend-server and associated CA are the only entities emitting certificates.

◀

Adding / deleting a doctor

A patient can add or remove a doctor to his list of appointed doctors. Note that this action can be initiated by the associated doctor himself, but then require explicit approval from the patient.

Viewing a medical record

Patients can view their own medical records at any time, as well as doctors who are appointed to them. No one else has access to these medical records.

Uploading, editing and deleting files from the server

A patient can submit a file to the server to be part of his medical record, which will be uploaded from its device. In the same way, a patient can overwrite the content of a file from his medical record, or delete it permanently.

Note that these actions can be initiated by a doctor appointed to the patient (the file is then uploaded from the doctor's device), but then require explicit approval from the patient.

4 Submission

Projects can be implemented in groups of arbitrary size, and submitted with the help of a gitlab[5] repository[6]. For that purpose, send us an email on ?? by 23:59 at the latest with the ssh URL[7] to your repository[8], and the name and matricule of your group members.

[5] The only two allowed instances are `gitlab.com` and `git.esi-bru.be`.

[6] Create the repository yourself, add your teachers (Ask your teacher for his id if you can't find it.) as maintainers.

[7] A gitlab ssh URL looks like `git@instance.com:username/projectname.git` .

[8] The automatic email notification is *not* enough.

You have to submit your work on ?? by 23:59 at the latest. The minimal requirements for submitted projects are as follows:

- projects have to be registered and submitted on time[9],
- projects have to provide a `README` file
  - mentioning the name and matricule of your group members,
  - explaining how to build[10] your project on a x64 ubuntu 22.04 distribution or a x64 Windows 10 machine (we recommend here to either provide a Makefile, or a shell script to install missing dependencies, compile the project and run relevant scripts),
  - explaining how to use your project (for example, "to launch the project, type the following command in a shell").

Projects failing to meet these requirements will not be graded (that is, they will get 0/20). In particular, projects that do not compile according to your *exact* instructions will not be graded. Furthermore, note that we shall in *no way* build or run your projects in an IDE.

Furthermore, if, at *any point*, you transmit or store sensitive data[11] to a server in plaintext, you will *fail hard*, regardless of any amount of work you may have done.

As usual, you must provide a modular code, easy to maintain, etc. Moreover,

- any submitted code must be duly documented and provide needed configuration files in order to produce the developer documentation.
- *only* compliance with this document and security-related aspects are graded for this project.

Master note: Furthermore, any submission must include a report under PDF format detailing your choices regarding security. You are strongly advised to follow the guidelines presented by H. Mélot [1] for your redaction, and to answer all questions listed in the check-list attached to this document. ◀

References

[1] H. Mélot. Éléments de rédaction scientifique en informatique. http://informatique.umons.ac.be/algo/redacSci.pdf - Consulté le October 16, 2025., 2011.

[9] We *strongly* insist: no delay of any kind shall be tolerated.
[10] It is expected that your script installs missing dependencies in addition to compiling your code.
[11] This means, among others, sensitive credentials, sensitive data or metadata, etc.