COS 330
Practical 1
Specification
Release Date: 04 August 2015 (16H30)
Due Date: 18 August 2015 (23H59)
Instructions
In this practical you are required to create an application that demonstrates your thorough understanding of computer security so far. You are allowed to use programming languages and technologies of your choice, as long as you can upload the application and download it from the CS website for demonstration, and as long as those applications work in the lab or virtual environment provided to you.

Note: The aim of this practical is NOT to test anything other than Computer Security concepts that you are expected to know by now.

Upload a zip archive of your code onto the CS website by the specified due date. If you do not demonstrate your program in one of the practical sessions, then you will not be allocated any marks (even if you did upload), i.e. you must be present in person at the demo session to be able to receive a mark.

*Everything that you submit might be checked for plagiarism. Instances of plagiarism will be dealt with in a serious manner.*

Background
In chapter 1 of the prescribed textbook you covered the theory behind *assets, vulnerabilities, threats, identification* and *authentication*. In chapter 2 you covered the three types of authentication mechanisms (*something you know, something you have and something you are*) and multi-factor authentication.

This practical will help you setup assets and protect them from unauthorized access (i.e. possible exploitation) with strong authentication. That is, only *duly authenticated* people must be allowed to gain access to the assets.
You can create any kind of application (web, stand-alone, mobile etc.) for this practical. The application should address all of the following requirements:

- Your application must contain a registration functionality to allow the identification of people that are able to access the assets.
- Registered users must have one of the access levels described below:
  - Level One: Read Permission
  - Level Two: Read/Write Permission
- The above mentioned access levels are in relation to files stored in your application (e.g. text files). They will serve as your assets.
- Your application must give users access based on their access levels.
- Your application must use two-factor authentication. You can combine any two authentication types.

**Note:** The usage of a framework that implements the specified requirements is not permitted. However, libraries can be used to help you with specific functionality. A fully working solution using two different types of authentication will earn 16 marks. Depending on the complexity of the solution and the chosen authentication mechanisms additional marks may be earned.