Design Project

Consider UTSA's network, which has many assets to protect:

- The computers in classroom, library, labs, etc.
- There are various kinds of sensitive information: employee data, student data (including grades)
- The access to the electronic library documents, such as electronic books

Suppose you are the CIO/CSO of UTSA. Your task is to design **security architecture** to protect UTSA's electronic assets and digital information. Please turn in a technical report, in .pdf (which can be made from .doc or Latex or other tools), that describes **your design of security architecture, by applying as much as possible what you learned from this class**. The content of the report should include:

- Section 1: Description of the design objectives (by elaborating the description given above, especially what you want to achieve, such as *confidentiality, integrity & availability* of student records)—essentially: what you want to accomplish?
- Section 2: Your Design and Security Analysis---essentially: how you propose to accomplish it and you argue that you indeed accomplished it
    - Section 2.1: Threat Model (what attacks you plan to defend against)
    - Section 2.2: Main Design (including your security architecture as well as the security mechanisms that are to be deployed within the architecture (including some figures that highlight ideas)
    - Section 2.3: Security Analysis (arguing, if not proving, how your design achieved the desired objectives)
- Section 3: Conclusion and Discussion (what conclusion you can draw; including possibly: the attacks that you want to defend against, but do not know how; how the knowledge scattered in other courses have been collectively used to some problems; what further knowledge needs to be learned in order to become a competent security architect)

Please note that this project is not trivial, because you need to systemize your knowledge that is learned from this class and other classes even beyond Computer Security.

Please note that extra credits will be given to ideas that are substantial and significant, such as:

- In your design, you used security mechanisms/techniques that are not learned in this class.
- In your security analysis, you can formally prove some properties (e.g., in cryptographic framework).

You must work on your own. You **cannot** discuss your design with your classmates. There is a lecture that is to be dedicated to clarify issues.

The grading criteria will include the following:

- Well-written and comprehensible **(5-10 pages, excluding cover page)**
- Includes strong arguments that the design realizes the objectives/specification
- Includes strong arguments that the security architecture is competent
- Includes strong arguments on the selection of security mechanisms