Assoc. Prof. Dr. Deniz Turgay ALTILAR
Assoc. Prof. Dr. Mustafa Ersel KAMAŞAK
Lect. Dr. Mehmet Tahir SANDIKKAYA

Task:

Implement a two-factor authentication mechanism for your smart phone.

In the context of this project, two-factor authentication is a mechanism to further secure an entity's log in to a computerized system by adding a second factor to the conventional passwords.

It is favored that, the second factor to biometrically identify the user (owner of the smart phone) is a statistical method that collects data from phone's surrounding. Four common examples are as follows: the voice of the user, the face of the user, the movements of the user, and the signature of the user.

Other than biometrically identifying the user, cryptographic second factors could be used. These are mainly based on a previously shared secret value (a long-term shared key composed of random bits) and cryptographic hash algorithms. You may refer to RFC 4226 for a more definitive example (https://tools.ietf.org/html/rfc4226).

Important Notes:

This project is designed to be prepared for 9 person×week. Thus, it is expected that students form groups of *exactly* three people to prepare this project. Please form the groups with two of your friends. The research assistants will note the groups on Monday, 25th September 2017 in the class.

There will be a question and answer session in the classroom on Monday.

Submission:

- Submit a technical **report** of your work. This report must include which factor you have chosen, the rationale behind your decision, design of your software, implementation steps and a discussion of possible security flaws and how your software avoids them.
- **Present** your work to the jury (composed of advisors and research assistants). Your presentation must defend your decisions, the major graces of your software design, and how your software mitigates security flaws in authentication.
- Submit the generated **code** and other relevant design **documentation** for inspection.

The code and documentation must be submitted in an archive file. The report must be a single pdf document. All submissions are done through Ninova system once per group. Presentations are conducted in the classroom in the designated session.