Despite almost 50 years of research in information security, systems still endure crescent challenges to fulfill security policies even the modest ones, such as confidentiality. Some of the problems can be reassembled due to the lack of use or the uncoordinated use of the best techniques and improvements in the information security area and cryptography in such systems.

In this course the students will be guided in the conception, the project, the implementation and a system evaluation (possibly embedded, involving hardware) with a security objective to be defined. The course approaches both theoretical and practical aspects and the students will be divided into teams, which each will have antagonist objectives: defense and attack.

The methodologies used will be similar to those employed in military and critical systems around the world. In order to achieve that, we will be hosting lectures from expert researchers in related themes (e.g. malwares, secure coding).

Your grade in this course will be given by your project grade, an exam and eventually some bonuses. Undergraduation and graduation students will be evaluated in distinct ways.

The project grade will be in range from 0 to +10. This grade will be based in the effectiveness of the protection offered by the system, in the quality and completeness of the security analysis, in the employment of project management techniques and usability, among other factors.

The exam grade will vary from -20 to +10. In the exam each question may have different weights (that means, worth different amount of points). Be X the weight of a question. If it’s answered with “don’t know”, it’s assigned 0 points. If it’s correctly answered, it’s assigned X points. If it’s incorrectly answered, it’s assigned -2X points. The sum of points will be your grade in the exam.
The eventual bonus points will be assigned to small projects or challenges proposed throughout the course.

The final **undergraduation** grade (from 0 to 10) will be given by:

\[
N_{\text{final}} = 0.8 \times N_{\text{project}} + 0.4 \times N_{\text{exam}} + \sum N_{\text{bonus}}
\]

The final **graduation** grade (from 0 to 10) will be given by:

\[
N_{\text{final}} = 0.8 \times N_{\text{project}} + 0.2 \times N_{\text{exam}} + \sum N_{\text{bonus}}
\]

**DATES**

- **Monitoring the project:** weekly or fortnightly. During a session the groups will do a brief presentation about the progress of their respective project activities and salient points will be discussed;
- **Partial delivery of the project and security analysis documentation:** 05/10/2015. This is the preliminary delivery of the system and its documentation. At this point the system should have its basic features working;
- **Deliver the final project and constructive documentation:** 02/11/2015. This is the main commit of the system and should contain, besides the system itself, the security analysis documentation, the implantation and the configuration in the validation environment. Also, the system must be completely functional. From this date on, the adversary will have direct access to the system;
- **Results of intrusion to the adversary system:** 18/11/2015. This is the main commit for the intrusion analysis of the system and should contain results regarding the intrusion of the adversary system, analysis document and artifacts which were employed/developed;
- **Post attacks adjustments:** 25/11/2015. This delivery shall include analysis results and any corrections due to the attacks perpetrated by the adversary(s);
- **Exam:** 30/11/2015;
- **Supplementary Exam:** 14/12/2015.