Formal Methods for Secure Systems course (A.Y. 2019-2020)

The exam is made up of a practical test and an oral test (using Google Meet).

The practical test consists in a project carried out in group on the application of one specific modelling/evaluation/verification technique to a cyber-security specific problem.

The project is carried out under the guidance of the teachers, and it must be completed and delivered to teachers at least one week before the examination.

The oral test consists of an interview. The student is requested to demonstrate his/her knowledge of the course material.

To attend the oral test, it is necessary to pass the practical test.

Practical test

Projects can be done by groups with no more than 4 persons.

Steps for the project:

1. Choice of the project topic and communication of the student names to the teacher
2. After approximately 1/3 of the expected duration of the project, review with the teacher of the current state of the project
3. After approximately 2/3 of the expected duration of the project, review with the teacher of the current state and initial results
4. Submission of the project one week before the oral exam
    - The project must be documented including the design choices
    - The code and the documentation must be submitted as a single zip file.

The project must be presented by the group in a single meeting (using a small set of slides) and the code must run correctly.
Each group component can do the oral test in different exam sessions

Project evaluation: unsatisfactory, satisfactory, good, very good.
Satisfactory is the minimum to be admitted to the oral test.
The evaluation is a bonus for the final mark.

Project

“Extend the ADVISE Bank Robbery case study and use Mobius to compute probability of success of attacks”

Mobius

Mobius is a tool for the analysis of availability, reliability and security of computer-based systems.

Objective of the project

Extend the ADVISE Bank Robbery model and assess the probability of the adversary to reach the goal with the new model.

“Extend the ADVISE Bank Robbery case study and use Mobius to compute probability of success of attacks”

Tasks

1. The students should introduce at least 10 new elements chosen among Access, Knowledge, Skill and Attack step. New goals can also be introduced.

2. Statistical analysis on the success of the attacks should be evaluated through simulation.

3. The extensions and the results of the analysis must be well documented. Students must be able to show results running Mobius during the exam (Mobius license).

Project
“Secure Information Flow by Model Checking”

Model Checking

Model checking tools support specification languages for modelling the behaviour of systems

Objective of the project

Model check the abstract semantics of Java bytecode against temporal logic formulae expressing the absence of data leakage

“Secure Information Flow by Model Checking”

Tasks

1. Use the open source symbolic model checker NuSMV (http://nusmv.fbk.eu/)
2. Implement the generation of the abstract transition system of a subset of the bytecode by using the formal specification language of NuSMV
3. Specify the logic formulae in the CTL language of NuSMV
4. Apply the method to check data leakage to a set of code fragments
5. Document the approach and the results of the analysis

Assume the following are given by the teacher:

- the subset of the bytecode and the abstract semantics rules (point 2)
- the set of code fragments to be analysed (point 4)

Project
“Data alteration attacks on Cyber-Physical Systems”

CPS

Cyber-Physical Systems are system composed of a plant component and a control component continuously exchanging data

Objective of the project

Assess the potential threat of data alteration attacks between control and plant sub-system

“Data alteration attacks on Cyber-Physical Systems”

Tasks

1. The students should simulate a Line follower robot (LFR) with four sensors, following the architecture learned during classes. The folder for the creation of the Control FMU with 4 inputs can be found here: https://drive.google.com/open?id=11qM_3ahwe6NCIwByPiLpsevQpt_LCusi
2. The students should introduce two malicious behaviors (data alteration attack) for each member of the team: one malicious behavior created by adding extra FMUs and one malicious behavior by changing the code of the controller. Within the same team, all the attacks should be different.
3. Document the malicious behaviors and the results of the analysis.