



NEOLAiA Focus Academy

Course Syllabus

Introduction to Information Security Requirements

Instructors

Shang Gao, Panagiota Chatzipetrou, Kai Wistrand, Örebro University Harald Gjermundrod, Ioanna Dionysiou, University of Nicosia Christian Esposito, University of Salerno

Overview and general information

One of the challenges in software system development is to understand information security requirements that need to be fulfilled. The focus of this course is how to analyze and evaluate information security requirements and to communicate these requirements with other relevant actors in the system development life cycle. Different methods for information security requirement engineering are covered. This course also develops students' skills in presenting information security requirements in both writing and speech. This course has been developed by instructors from three universities within the NEOLAiAAlliance: Örebro University, the University of Nicosia, and the University of Salerno and will address the NEOLAiA Pillar of Digital Transformation

Objectives

The main objectives of the course are:

- 1. Understand foundational concepts of requirements, requirements engineering processes, and information security requirements.
- 2. Apply requirement engineering modeling techniques to identify and model information security requirements.
- 3. Analyze the relevance of defining information security requirements within different phases of the system development life cycle.
- 4. Develop written communication skills to effectively present information security requirements
- 5. Develop oral communication skills to effectively present information security requirements

Learning outcomes and competencies

After completed studies, the students should

- have basic understanding of the concepts of requirements, requirement engineering processes, and information security requirements
- have basic ability to identify and model information security requirements based on requirement engineering modelling techniques
- have a basic ability to analyze when and where it is appropriate to define information security requirements based on an understanding of the system development life cycle
- have basic skills in presenting information security requirements in both writing and orally

Contents

The course contents consist of the following components:

- Introduction to system development life cycle
- Introduction to the concepts of requirements and information security requirements

NEOLAIA - WP2 Improving Teaching and Learning





- Modeling Information security requirements with misuse case modeling
- Basic oral and text presentation practices in the academic context

Number of students, profile, selection process, and registration

The plan is to enroll 40 students in this course. The prerequisite for enrolling in this course is to have 30 credits in Informatics or the equivalent. To be eligible for the course, students should be enrolled at a university that is either part of the European Universities alliance, NEOLAiA, or an ERASMUS+ partner university with which Örebro University's Informatics department has an Erasmus agreement. Each university can nominate up to 10 students. First, each participating university will select its international students locally and rank them based on their grades or ECTS points. Then, Örebro University will finalize the student selection by considering the rankings provided by all participating universities, and available spots. Lecturers from Örebro University, along with guest lecturers from some of the participating universities, will be responsible for on-site teaching. The course will also include remote sessions.

Activities

The following activities will be available to students, staff, and faculty: recorded lectures, literature readings, group work, workshops, group presentations, guest lectures and social activities. Additionally, an on-site panel session will be open to students, staff, faculty, and the wider community.

Calendar/program

Please refer to the following website for the course schedule. <u>https://www.oru.se/english/schools/Orebro-University-School-of-Business/student-information/introduction-to-information-security-requirements/</u>

Assessment

Oral Presentation, 1 credits (Addresses course objective 1,2,3,5) Written Report, 2 credits (Addresses course objective 1,2,3,4) The grades for both oral presentation and written report, as well as the final grades for this course, are: Fail (F), Sufficient (E), Satisfactory (D), Good (C), Very Good (B) or Excellent (A).

Additional comments

The course syllabus is available at the following website:

https://api.oru.se/oruapi/v1/utbildningsinformation/utbildning/IK230G?revision=1%2c&accept=ht ml&sprak=en&typ=kurs&apikey=m2zu4QyMfr9hDP65XgjAhJGttFhM5jxYPXke6Vydftl29Z5loFzyG7d pyMcMnihi

The students will receive grades and course certificates in accordance with Örebro University's standard procedures.

NEOLAIA - WP2 Improving Teaching and Learning

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.





References

- Gürses Seda, Magali Seguran & Nicola Zannone Requirements engineering within a largescale security-oriented research project: lessons learned Requirements Engineering 18.1 (2013): 43-66
- Hope Poco, McGraw Gary & Annie I. Antón Misuse and Abuse Cases: Getting Past the Positive IEEE Security & Privacy 2004; May/June:32-4
- Pohl, Klaus (2010) Requirements engineering: fundamentals, principles, and techniques Springer Publishing Company, Incorporated
- Røstad, Lillian An extended misuse case notation: Including vulnerabilities and the insider threat 12th International Working Conference on Requirements Engineering: Foundation for Software Quality (REFSQ'2006); 5 June, 2006 Luxembourg, Luxembourg2006. p. 33-43
- Sindre, Guttorm & Andreas Lothe Opdahl Eliciting security requirements with misuse cases Requirements Engineering 2005; 10(1):34-44