Exchange programme Vrije Universiteit

Vrije Universiteit Amsterdam - Exchange programme Vrije Universiteit - 2022-2023

Exchange

Vrije Universiteit Amsterdam offers many English-taught courses in a variety of subjects, ranging from arts & culture and social sciences, neurosciences and computer science, to economics and business administration.

The International Office is responsible for course approval and course registration for exchange students. For details about course registration, requirements, credits, semesters and so on, please visit the exchange programmes webpages.

Security and Safety Engineering

Course Code	XB_0088
Credits	6.00
Period	P4
Course Level	200
Language Of Tuition	English
Faculty	Faculty of Science
Course Coordinator	prof. dr. ir. F. Massacci
Examiner	prof. dr. ir. F. Massacci
Teaching Staff	dr. K. Tuma, prof. dr. ir. F. Massacci, F. Minna, W.B. Mbaka, A. Papotti, S. Kanwal, dr. F. Madeiral Delfim
Teaching method(s)	Partial Exam, Lecture, Seminar

Course Objective

This course is an introduction to security and safety engineering for Bachelor Students in Computer Science to:

(i) build awareness of security and safety issues in software systems,
(ii) apply security and safety threat analysis and mitigation techniques at conceptual level to simple case studies, and
(iii) inspire students to further their education in computer security.

Course Content

After completing this course, the student will be able to:
- Describe the conceptual elements of security and safety engineering in terms of assets, threats, vulnerabilities, security mitigations, and risks. [Knowledge and understanding, Communication]
- Explain the role of security and safety analysis techniques in addressing security and safety problems in IT systems. [Making judgements, Communication]
- Apply qualitative security and safety engineering techniques on a concrete problem instance and explain the rationale of the proposed solution. [Applying knowledge and understanding, Making judgements, Communication]
- Identify and review pros and cons of qualitative techniques for solving a concrete problem instance. [Knowledge and understanding, Lifelong learning skills]
- Apply industrial assessment techniques for a concrete problem instance in the case of software vulnerabilities and systems. [Applying knowledge and understanding, Lifelong learning skills]

Additional Information Teaching Methods

The course is organized over the principle of active learning.
- Class lectures introducing the topic
- Assignments in the form of a report analyzing and reflecting on the result
- Class discussions on the assignments
- Peer review of the reports of the other groups
- Feedback on the peer review
- Assessment of software vulnerabilities based on industry standards

The lectures will cover asset & risk analysis, safety and security analysis, identification of conceptual threats and security mitigations, software vulnerability and IT system assessment.

Assignments are due in intermediary incremental submissions (on a weekly

basis).

To provide intermediate progress feedback and to learn to identify and review the application of the technique to a case study, a random sample of the assignments will be presented to the entire class for discussion. Students of the sampled deliverables will be asked to present the rationale in class. All students will be asked to present their finding to their peers.

All students will then peer review the submissions of the other groups following the rubric identified during the review.

Method of Assessment

POSITIVE points will be assigned with the following grading scheme:
+ 10% active participation in the peer review process.
+ 10% evaluation of the first report as performed by your peers
+ 15% evaluation of the second report as performed by your peers.
+ 20% evaluation of the third report as performed by your peers.
+ 25% evaluation of the fourth report as performed by your peers.
+ 20% assessment of software vulnerabilities according to industry standards

NEGATIVE multiplier points
Negative multiplier points will be obtained when failing the discussion as detailed
below. When a student fails to show up for the discussion or fail to explains what is in the report and why it is in the report, or fail to modify code used to compute the results reported in the report, s/he will take a negative grade for the report submitted. For example, a report positively graded 8.5 will be counted -8.5 towards the final grade.

PASS OR FAIL
– quality of the reviews as graded by your peers and re-evaluated by the lecturer. Students who fail this part due to extremely poor or unfair reviews will be asked to provide comprehensive qualitative analysis of the reports submitted by the other students as a resit.

All points for the assignments will be normalized so that the best submitted report will be graded 10/10 (or -10/10).

RESIT
- A final report of a different case study can be resubmitted as a partial resit for one of the assignments
- Students who fail the reviewing part will be asked to provide comprehensive qualitative analysis of the reports submitted by the other students as a resit using Atlas.ti

Literature

Gibson. Managing Risk in Information Systems. Jones & Bartlett
This book offers a general structure of the security assessment process in industry and can be followed for the high level process of threat and security
Anderson. Security Engineering. Wiley.
The previous version of the book is available on line
https://www.cl.cam.ac.uk/~rja14/book.html
Shostack, A. (2014). Threat modelling: Designing for security. Wiley
Selected chapters will be made available on canvas for educational use.

Additional Information Target Audience

Computer Science Bachelor (year 2)

Additional Information

To avoid a negative grade is not important if the report is actually wrong (report correctness is evaluated by the peer review). It is important that a student can explain why s/he wrote what is written in what is his/her report. The purpose of an honest discussion is precisely to clarify doubts and mistakes. As a side effect it can serve as control of plagiarism and free riding.

EXAMPLE of interaction
“Report says on page 3 “Our security controls must show ecological validity…” [Entire sentence actually copy and pasted from a web page]
Lecturer’s question: “Why must your security controls show ecological validity?
-- IF student’s answer is “What is ecological validity?” THEN fail (=won a minus grade)
-- ELSE IF answer: “I didn’t write that, X did” THEN fail (=won a minus grade)
-- ELSE IF answer is “I took it from the web site Z.”
---- Second question: “Let’s ignore that you should have written it was from Z, why is it applicable to you?”
---- IF second answer is “I don’t know.” THEN fail (=won a minus grade)
---- ELSE the answer is “This is important because we must show that developers can apply the controls in their work environment”
------- Second question: “But you have no developers here, you are comparing ML tools, how would you change the security controls?”
------- Student Answer is “Aha. We need to [some technical explanation]”
------- Lecturer follow-up:”This might not fully work because [follow technical explanation why this is wrong or right] Let’s see what somebody else thinks.“

Custom Course Registration

Students should register on CANVAS at least four weeks before the course starts. Groups will be done in Canvas.

Explanation Canvas

The peer review of the reports will be done in Canvas.

Recommended background knowledge

Students should have the background knowledge provided by the courses on Software development, Computer Networks and Operating Systems.