lingi2144

2019

Secured systems engineering

In view of the health context linked to the spread of the coronavirus, the methods of organisation and evaluation of the learning units could be adapted in different situations; these possible new methods have been - or will be - communicated by the teachers to the students.

5 credits	30.0 h + 15.0 h	Q2

Teacher(s)	Legay Axel ;
Language :	English
Place of the course	Louvain-la-Neuve
Main themes	The goal of this course is to learn how to build a secure application from theory to practice in a production environment. As a case study, we will focus on token-based applications whose primary goal is to ensure authentication. • Introduction to cyber security and virology • Threat Vulnerabilities and Attack • Vulnerability of C language (Buffer overflow, heap, format string) and protections • Shell code: write in C / assembler • Malware classification • Malware detection • Static, dynamic and artificial intelligence techniques.
Aims	Given the learning outcomes of the "Master in Computer Science and Engineering" program, this course contributes to the development, acquisition and evaluation of the following learning outcomes: • INFO1.1-3 • INFO2.1-5 • INFO5.2, INFO5.4-5 • INFO6.1, INFO6.3, INFO6.4 Given the learning outcomes of the "Master [120] in Computer Science" program, this course contributes to the development, acquisition and evaluation of the following learning outcomes: • SINF1.M1 • SINF2.1-5 • SINF5.2, SINF5.4-5 1 • SINF6.1, SINF6.3, SINF6.4 Students completing successfully this course will be able to • design secure IT systems • implement a secure application based on and test the security of existing application • Explain the security techniques and tools used in order to convince potential users that these aspects have been properly taken into account. Students will have developed skills and operational methodology. In particular, they have developed their ability to • take into account the ethical dimensions in their professional practice, • argue that IT tools are becoming commonplace and that this creates risks in terms of information security and, in particular, the protection of privacy. - - - - *The contribution of this Teaching Unit to the development and command of the skills and learning outcomes of the programme(s) can be accessed at the end of this sheet, in the section entitled “Programmes/courses offering this Teaching Unit”.*
Evaluation methods	**Due to the COVID-19 crisis, the information in this section is particularly likely to change.** **On first session:** • an exam for 60% of the final mark • two works for 40% of the final grade **In second session**: An exam that counts for 100% of the final grade.

Teaching methods	**Due to the COVID-19 crisis, the information in this section is particularly likely to change.** Theory classes, practical classes. Seminar by external experts.
Content	The objective of the course is to give an introduction to software security. We will first discuss the concepts of security and software attack. We will then analyze software vulnerabilities and we will study protections. Finally, an introduction to malware analysis will be presented. Content: - Introduction to cyber security - Introduction to notions of vulnerabilities, threats and attacks - Introduction to fishing - Introduction to privilege escalation - Integer overflow - Buffer overflow: assembler, protection and counterattack - String format and vulnerabilities of C language - Writing of "shellcode" - Introduction to static and dynamic analysis of malware - Honey pots - Dynamic memory analysis - Packing and cracking - External stakeholders: security at UCLouvain, at CISCO and at NVISO. - Practical exercises on computers - Lab: setting up traps, intrusion, malware analysis
Inline resources	https://moodleucl.uclouvain.be/enrol/index.php?id=12241
Bibliography	Available on moodle. Disponible sur moodle.
Other infos	INGI2347 vs INGI2144 • INGI2347 is an introduction to network and application security. • INGI2144 is an advanced course on application security. Background : • computer systems and programming. It is not necessary to follow INGI2347 in order to follow INGI2144 • Students who do no know whether their background allows them to attend the course (e.g. students from ELEC, ELME or MAP) should contact the lecturer.
Faculty or entity in charge	INFO

Programmes containing this learning unit (UE)

Program title	Acronym	Credits	Prerequisite	Aims
Master [120] in Data Science Engineering	DATE2M	5		🔍
Master [120] in Computer Science and Engineering	INFO2M	5		🔍
Master [120] in Mathematical Engineering	MAP2M	5		🔍
Master [120] in Computer Science	SINF2M	5		🔍
Master [120] in Electrical Engineering	ELEC2M	5		🔍
Master [120] in Data Science: Information Technology	DATI2M	5		🔍