UCLouvain

linfo2144

2026

Secured systems engineering

5.00 credits	30.0 h + 15.0 h	Q2

Language :	English > French-friendly
Place of the course	Louvain-la-Neuve
Prerequisites	Required#: skills in C programming language as taught in course LEPL1503 Required#: principles of computer systems, as targeted in course LINFO1252
Main themes	This course introduces software security by exploring the fundamentals of cybersecurity, software attacks, and vulnerabilities, such as those found in cryptographic protocols, RFID cards, and biometric passports. Students will examine techniques for protecting against attacks and gain familiarity with malware analysis. Advanced topics include integer and buffer overflows, static and dynamic malware analysis, and practical exercises involving setting traps and analyzing intrusions and malware.
Learning outcomes	**At the end of this learning unit, the student is able to :** 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 • INFO5.3-5 • INFO6.1,6.4-5 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 • SINF5.2-6 • SINF6.1,6.4-5 Students completing successfully this course will be able to: • Analyzing the security of applications by identifying and assessing security risks, searching for vulnerabilities in code, designing and applying methodologies to ensure the absence of security flaws; • Understanding and analyzing malware as well as aspects of operational security; • Designing and analyzing systems using authentication mechanisms while ensuring the security of these systems; Students will have developed methodological and operational skills. In particular, they will have strengthened their ability to: • write a concise technical report on the security of an application, appropriately using terminology and theoretical concepts; • implement a secure solution by applying best development practices; • develop tools for evaluating the security of an application or protocol and, where applicable, exploiting a vulnerability; • consider ethical dimensions (particularly regarding privacy, confidentiality of information, etc.) in their professional practice; • argue about the widespread use of computing tools and the security risks it entails, especially concerning privacy protection.
Evaluation methods	Evaluation for the **June session**: • Written exam (70% of the final mark) • Oral assessment of practical session during the quadrimester (30% of the final mark) Evaluation for the **August session**: • Written exam (100% of the final mark)
Teaching methods	Lectures, Literature reading, Practical session
Content	The course offers an introduction to IT system security through a variety of topics. Examples of topics covered in previous years:

	• Privilege escalation and separation. • Memory security (buffer overflow, stack overflow, exploits on dynamic memory allocations): attacks and countermeasures; undefined behaviour. • Static and dynamic malware analysis. • Design of secure communication protocols (example: TLS). • Machine authentication systems: cryptography fundamentals, certificates, TOFU, etc. • User authentication: password security, multi-factor authentication, single sign-on (SSO). • Software supply chain: secure distribution, updates, dependencies, traceability. • Incident response
Inline resources	https://moodle.uclouvain.be/course/view.php?id=3593
Bibliography	Available on moodle. Disponible sur moodle.
Other infos	INFO2144 vs INFO2347: • INFO2144 is a course that explores the above topics in greater depth. • INFO2347 is a general introduction to cybersecurity, with a particular focus on network and web application security. Prerequisite(s): • A general knowledge of computer systems and programming is required. It is not necessary to take INFO2347 in order to take INFO2144.
Faculty or entity in charge	INFO

Programmes containing this learning unit (UE)

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