UCLouvain

linfo2144

2022

Secured systems engineering

5.00 credits	30.0 h + 15.0 h	Q2

Teacher(s)	Legay Axel ;
Language :	English > French-friendly
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 token-based applications. • RFID Primer: current applications and characteristics. • Symmetric Key Authentication Protocols. • Examples of poor designs (MIT, DST), TMTO. • Implementation of cryptographic building blocks • Generating randomness. • Examples of poor designs (Mifare). • Relay attacks and distance bounding. • Privacy: Information leakage and malicious traceability. • Denial of Service. • Study case the biometric passport.
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 • INFO5.2, 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 • SINF6.1, SINF6.3, SINF6.4 1 Students completing successfully this course will be able to • design of computer systems using the authentication token ensuring the security of these systems, • implement a secure token-based application whose main objective is to provide authentication , • explain the techniques used in security 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 • write a brief technical report to highlight the main features of software that has been developed , utilizing the proper terminology and the appropriate theoretical concepts , • achieve a successful demonstration of the software that has been developed , choosing the relevant tests according to the specifications and ensuring in advance that the software passes them , • consider the ethical dimensions (particularly regarding respect for privacy , confidentiality of information , ...) as part of their professional practice , • argument to the commoditization of computer systems and risks that this entails in terms of information security and in particular for the protection of privacy .

Evaluation methods	**On first session:** • an exam for 60% of the final mark • two works for 40% of the final grade Students who obtained at least 12/20 for the two works can be exempted from the oral exam. **In second session**: An oral exam which counts for 60% of the mark. The 40% of the work obtained in the first session cannot be redone and is kept for the second session.
Teaching methods	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	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		