UCLouvain

lingi2347

2020

Computer system security

Due to the COVID-19 crisis, the information below is subject to change, in particular that concerning the teaching mode (presential, distance or in a comodal or hybrid format).

5 credits	30.0 h + 15.0 h	Q2

Teacher(s)	Sadre Ramin ;
Language :	English
Place of the course	Louvain-la-Neuve
Main themes	• Forged E-Mail, Spam and Malwares, • Basics in cryptography, • Network and Application Vulnerabilities: IT spoofing, session hijacking, exploits, sniffing, • Firewalls, • Proxies, IDS, Hacking methods, • Secure communications, • Security at the User Level.
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, INFO4-5 • 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, SINF4-5 • SINF6.1, SINF6.3, SINF6.4 The course provides a broad view of computer system security that provides a general knowledge of the field for non - specialists and a base for future specialists. Students completing successfully this course will be able to • defend the need for protection and security, and the role of ethical considerations in computer use, • identify security strengths and weaknesses in computer systems, • explain the problems addressed by digital forensics and outline the basic principles involved in its practice, • compare and contrast current methods for implementing security. 1 - - - - *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.** Envisaged mode of evaluation: • Projects (35% of the final mark) • Exam (65% of the final mark) Depending on the circumstances and the number of participating students or other reasons, modifications to the evaluation plan can happen, for example replacing the written exam by an oral exam or a second project. In case of doubt, the teacher reserves the right to test some students in an additional oral exam that complements or replaces the grade obtained in the project(s) and/or the written exam.
Teaching methods	**Due to the COVID-19 crisis, the information in this section is particularly likely to change.** The course consists of a series of lectures and accompagning exercises and project(s). The teaching method can change depending on the circumstances and the number of participating students or for other reasons. Face-to-face classes as well as remote teaching or a mix of the two methods are possible.

Content	The course covers a wide spectrum of the security problems related to computer systems and principles of building secure systems. This course will introduce fundamentals of computer security and applied cryptography. Topics include software vulnerabilities, malware, security in web applications, networking and wireless security, and applied cryptography.
Inline resources	Moodle
Bibliography	Livres de références non obligatoires • Introduction to Computer Security' by Michael Goodrich & Roberto Tamassia (ISBN-10: 0321512944, ISBN-13: 9780321512949) • Security Engineering: A Guide to Building Dependable Distributed Systems' 2nd ed. by Ross J. Anderson (ISBN-10: 0470068523, ISBN-13: 978-0470068526) Support obligatoire: transparents en ligne sur le site du cours sur Moodle
Other infos	INGI2347 vs INGI2144 • Class INGI2347 is an introductory to computer system and network security, while class INGI2144 is an advanced course on application security. Background: • LINGI2141 or eventually LELEC2920 : Background in computer networks • LFSAB1402 : Basic knowledge in programming • INFO2MS and SINF2MS students are both compliant with these prerequisites. Student who do not know if their background allows them the attend the course (e.g. students from ELEC, ELME or MAP) should contact the teaching assistant or lecturer. • Weaknesses in network can be filled by reading the book "Computer Network" by Andew Tanenbaum. The most important topics that will be used in INGI2347 are: SMTP, Telnet, IP, TCP, ARP, MAC, OSI layered model.
Faculty or entity in charge	INFO

Force majeure

Evaluation methods	Depending on the public health conditions during the exam period, the evaluation can take different forms: • Group project(s) (35% of the final mark) during the quadrimester and a written (face-to-face) exam during the exam session (65% of the final mark) or • Group project(s) (35% of the final mark) during the quadrimester and an individual projet during the exam session (65% of the final mark)

Programmes containing this learning unit (UE)

Program title	Acronym	Credits	Prerequisite	Aims
Master [120] in Computer Science and Engineering	INFO2M	5		
Master [120] in Computer Science	SINF2M	5		
Master [120] in Electrical Engineering	ELEC2M	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		