




Teacher(s)	Legay Axel ;
Language :	English
Place of the course	Louvain-la-Neuve
Main themes	<p>The objective of the course is to make the student aware of the problem of computer security by adopting the "ethical hacking" approach.</p> <p>The approach followed is that of showing how the vulnerabilities of a computer system can be exploited to threaten security. From there, the student will develop the skills necessary to detect these vulnerabilities and to protect the system. These can be deployed upstream or downstream (depending on the development process). We will also look at the cost and strength of these measures.</p> <p>The student will also receive a very brief introduction to malware analysis and the techniques to detect them.</p> <p>During this course, the student will also be aware of the place that cybersecurity takes in industry, as well as the ethical issues that are related to this field.</p> <p>For information, the vulnerabilities addressed will be: buffer overflow, integer overflow, format string, data race. Among the protection we will study the technique of the non-executable stack or even that of the "canary". For malware analysis, we will focus on MIRAI and the YARA tool.</p>
Aims	<p>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:</p> <ul style="list-style-type: none"> <li>• INFO1.1-3</li> <li>• INFO2.1-5</li> <li>• INFO5.2, INFO5.4-5</li> <li>• INFO6.1, INFO6.3, INFO6.4</li> </ul> <p>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:</p> <ul style="list-style-type: none"> <li>• SINF1.M1</li> <li>• SINF2.1-5</li> <li>• SINF5.2, SINF5.4-5</li> <li>• SINF6.1, SINF6.3, SINF6.4</li> </ul> <p>1 Students completing successfully this course will be able to</p> <ul style="list-style-type: none"> <li>• design of computer systems using the authentication token ensuring the security of these systems,</li> <li>• implement a secure token-based application whose main objective is to provide authentication ,</li> <li>• explain the techniques used in security in order to convince potential users that these aspects have been properly taken into account,</li> </ul> <p>Students will have developed skills and operational methodology . In particular , they have developed their ability to</p> <ul style="list-style-type: none"> <li>• 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 ,</li> <li>• 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 ,</li> <li>• consider the ethical dimensions ( particularly regarding respect for privacy , confidentiality of information , ...) as part of their professional practice ,</li> <li>• 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 .</li> </ul> <p>-----</p> <p><i>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".</i></p>
Evaluation methods	<p><b>On first session:</b></p> <ul style="list-style-type: none"> <li>• an exam for 60% of the final mark</li> <li>• two works for 40% of the final grade</li> </ul> <p><b>In second session:</b> An exam that counts for 100% of the final grade.</p>

Teaching methods	Lectures introduce the theoretical and practical background needed to build a secure token-based application.
Content	<p>The current attractive way to perform authentication with token is to use the RFID technology. Several billion RFID devices are sold every year and no one engineer should ignore this technology, its nice features, but its security flaws as well. To illustrate the course, we will see how to break an access card, a biometric passport, how to steal a car while being 20'000 km far from it, etc.</p> <p>From this technology, the course will describe and extend the main points one should take care when designing a secure application.</p> <p>Develop from scratch a secured solution.</p> <ul style="list-style-type: none"> <li>• How to read a standard.</li> <li>• Implement cryptographic tools.</li> <li>• Consider the solution as a whole.</li> <li>• ...</li> </ul> <p>Discover a new field: ubiquitous computing, especially RFID.</p> <ul style="list-style-type: none"> <li>• Everyday life applications based on RFID.</li> <li>• Several billions computing devices around us.</li> <li>• Computer science is no longer only PCs interconnected.</li> <li>• ...</li> </ul>
Inline resources	<a href="https://moodleucl.uclouvain.be/enrol/index.php?id=12241">https://moodleucl.uclouvain.be/enrol/index.php?id=12241</a>
Bibliography	Support obligatoire: copie des diapositives disponible sur le site icampus.
Other infos	<p>INGI2347 vs INGI2144</p> <ul style="list-style-type: none"> <li>• INGI2347 is an introduction to network security and IT applications.</li> <li>• INGI2144 is an advanced course on application security.</li> </ul>
Faculty or entity in charge	INFO

Programmes containing this learning unit (UE)				
Program title	Acronym	Credits	Prerequisite	Aims
Master [120] in Computer Science and Engineering	INFO2M	5		
Master [120] in Electrical Engineering	ELEC2M	5		
Master [120] in Computer Science	SINF2M	5		
Master [120] in Mathematical Engineering	MAP2M	5		