UCLouvain

lelec2770

2023

Privacy Enhancing technology

5.00 credits	30.0 h + 30.0 h	Q1

Teacher(s)	Pereira Olivier ;Peters Thomas (compensates Pereira Olivier) ;Standaert François-Xavier ;
Language :	English > French-friendly
Place of the course	Louvain-la-Neuve
Prerequisites	Familiarity with the basic notions of cryptography is welcome
Main themes	The exact course topics will change from year to year. Examples of relevant topics include techniques that make it possible to : • compute on encrypted data; • build a database that can be queried without the server knowing which parts of it are accessed; • have anonymous communications; • make digital cash; • shuffle cards over the internet; • organize an election in which the organizers can't cheat; • have services with access control that keep users untraceable; • understand attacks against privacy, including de-anoymization/re-identification attacks, profiling, data mining and side-channel attacks; • identify privacy issues related to mass surveillance and solutions to prevent them.
Learning outcomes	**At the end of this learning unit, the student is able to :** Based on the LO referential of the program « Master in Electrical Engineering », this course contributes to the development, acquisition, and evaluation of the following learnging outcomes : • AA1.2, AA1.3, • AA2.2, AA2.3, AA2.5, • AA3.1, • AA5.1, AA5.3, AA5.4, AA5.6, 1 • AA6.1, AA6.2, AA6.3 **Specific learning outcomes of the course** • At the end of this class, the student will be able to : • Analyze the risks of attacks against correctness and privacy for a concrete system • Understand cryptographic and architectural tools allowing to mitigate privacy issues • Evaluate utility and privacy metrics for databases and distributed systems
Evaluation methods	The final examination is based on exercises, based on the learning outcomes listed above. One of more mini-projects may be proposed during the semester and may contribute for at most 20% to the final grade. In any case, the grade of the mini-projects would only contribute to the final grade if it is beneficial to the grade. The exam of the January session is open-book, while the exam of the August session is closed-book. Details are available on Moodle.
Teaching methods	Lectures and exercise sessions. Homeworks and mini-projects may be proposed during the semester.
Content	Various themes will be discussed each year. These themes may include: secure two-party and multi-party protocols, oblivious memories, verifiable voting, crypto-currencies, verifiable computation, anonymous credentials, differential privacy and big data, post-Snowden cryptography.
Inline resources	https://moodle.uclouvain.be/course/view.php?id=3249
Faculty or entity in charge	ELEC

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		