UCL Université catholique de Louvain

LINGI2144

2012-2013

Secured systems engineering

5.0 credits	30.0 h + 15.0 h	1q

Teacher(s) :	Avoine Gildas ;
Language :	Anglais
Place of the course	Louvain-la-Neuve
Prerequisites :	Background in computer systems and programming is required. Students should have an general background in information security as provided by INGI2347. 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.
Main themes :	-- 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.
Aims :	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. 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. *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 :	Exam -- Written for the fist session, oral for the second session -- Documents allowed (with restrictions). Allowed: printed slides and personal notes. Except slides, documents not authored by the student are not allowed. No electronic device allowed. Grade -- First session: 35 % project + 65 % exam -- Second session: if the project is worse than the exam, it will not be taken into account in the final grade
Teaching methods :	-- Lectures introduce the theoretical and practical background needed to build a secure token-based applcation. -- Students are required to achieve a project in group of 3 over the whole semester, that is taken into account into the grade. Topic of the project is defined in September. -- Two laboratory sessions to discover the basic technics and the hardware used in the project
Content :	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. From this technology, the course will describe and extend the main points one should take care when designing a secure application. Develop from scratch a secured solution. -- How to read a standard. -- Implement cryptographic tools. -- Consider the solution as a whole.

	-- ... Discover a new field: ubiquitous computing, especially RFID. -- Everyday life applications based on RFID. -- Several billions computing devices around us. -- Computer science is no longer only PCs interconnected. -- ...
Bibliography :	Mandatory material: slides available on icampus.
Other infos :	INGI2347 vs INGI2144 -- INGI2347 is an introduction to network and application security. -- INGI2144 is an advanced course on application security.
Cycle and year of study :	> Master [120] in Electrical Engineering > Master [120] in Computer Science and Engineering > Master [120] in Computer Science > Master [120] in Mathematical Engineering
Faculty or entity in charge:	INFO