LINGI2144

2016-2017

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
Inline resources:	> http://icampus.uclouvain.be/claroline/course/index.php?cid=INGI2144
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.
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, 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 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 :	Homework The homework should be done by groups of two students. Exam - First and second sessions exams are written exam. - Documents and electronic devices are strictly forbidden during the exam. Final Grade The final grade is Max(exam, 14/20 exam + 6/20 homework)
Teaching methods :	Lectures introduce the theoretical and practical background needed to build a secure token-based applcation.
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. Background : -- computer systems and programming. 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.
Faculty or entity in charge:	INFO

Programmes / formations proposant cette unité d'enseignement (UE)

Intitulé du programme	Sigle	Credits	Prerequis	Acquis d'apprentissage
Master [120] in Mathematical Engineering	MAP2M	5	-	🔍
Master [120] in Electrical Engineering	ELEC2M	5	-	🔍
Master [120] in Computer Science	SINF2M	5	-	🔍
Master [120] in Computer Science and Engineering	INFO2M	5	-	🔍