UCL Université catholique de Louvain

LINGI2144

2014-2015

Secured systems engineering

5.0 crédits	30.0 h + 15.0 h	1q

Enseignants:	Avoine Gildas ;
Langue d'enseignement:	Anglais
Lieu du cours	Louvain-la-Neuve
Ressources en ligne:	> http://icampus.uclouvain.be/claroline/course/index.php?cid=INGI2144
Thèmes abordés :	L'objectif de ce cours est d'apprendre à construire une application sécurisée de la théorie à la pratique. Comme étude de cas, le cours se focalise sur les applications basées sur des cartes sans contact dont l'objectif principal est d'assurer l'authentification. -- Introduction aux applications basées sur descartes à puce. -- RFID: applications actuelles et les caractéristiques. -- Protocoles d'authentification, clé secrète et publique -- Exemples de mauvaises conceptions (MIT, DST), TMTO. -- Mise en place de primitives cryptographiques. -- Implémentation de générateurs de nombres pseudo-aléatoires. -- Exemples de mauvaises conceptions (Mifare). -- Attaques relais et test de proximité. -- Confidentialité: fuite d'information et traçabilité malveillante. -- Déni de service. -- Cas du passeport biométrique.
Acquis d'apprentissage	Eu égard au référentiel AA du programme « Master ingénieur civil en informatique », ce cours contribue au développement, à l'acquisition et à l'évaluation des acquis d'apprentissage suivants : -- INFO1.1-3 -- INFO2.1-5 -- INFO5.2, INFO5.4-5 -- INFO6.1, INFO6.3, INFO6.4 Eu égard au référentiel AA du programme « Master [120] en sciences informatiques », ce cours contribue au développement, à l'acquisition et à l'évaluation des acquis d'apprentissage suivants : -- SINF1.M1 -- SINF2.1-5 -- SINF5.2, SINF5.4-5 -- SINF6.1, SINF6.3, SINF6.4 Les étudiants ayant suivi avec succès ce cours seront capables de: -- concevoir des systèmes informatiques utilisant l'authentification par cartes sans contact en assurant la sécurité de ces systèmes -- implémenter une application sécurisée basée sur des cartes sans contact dont l'objectif principal est d'assurer l'authentification. -- expliciter les techniques utilisées en matière de sécurité afin de convaincre les utilisateurs potentiels que ces aspects ont correctement été pris en compte.

	Les étudiants auront développé des compétences méthodologiques et opérationnelles. En particulier, ils auront développé leur capacité à -- rédiger un rapport technique succint sur la sécurité d'une application en utilisant à bon escient la terminologie et les concepts théoriques, -- réaliser une implémentation d'une solution sécurisée, -- prendre en compte les dimensions éthiques (en particulier en matière de respect de la vie privée, de confidentialité des informations, ...) dans le cadre de leur pratique professionnelle, -- argumenter de la banalisation des outils informatiques et des risques que cela engendre en matière de sécurité de l'information et en particulier en matière de protection de la vie privée. *La contribution de cette UE au développement et à la maîtrise des compétences et acquis du (des) programme(s) est accessible à la fin de cette fiche, dans la partie « Programmes/formations proposant cette unité d'enseignement (UE) ».*
Modes d'évaluation des acquis des étudiants :	Examen -- écrit en première session, oral en seconde session -- Documents autorisés (avec restrictions). Admis: copies des diapositives et des notes personnelles. A l'exception des diapositives, tout document dont l'étudiant n'est pas l'auteur n'est pas autorisé. Aucun dispositif électronique n'est admis. Note finale -- Première session: 35% projet + 65% examen -- Deuxième session: si le projet est moins bon que l'examen, il ne sera pas pris en compte dans la note finale
Méthodes d'enseignement :	-- Cours magistral pour introduire les bases théoriques et pratiques nécessaires pour construire une application sécurisée basée sur des cartes sans contact. -- Projet qui s'étend sur l'ensemble du semestre et qui est réalisé par groupe de 3. Le sujet du projet est défini en Septembre. -- Deux séances en laboratoire pour appréhender les techniques de base et le matériel utilisé dans le cadre du projet.
Contenu :	La tendance actuelle pour faire de l'authentification avec carte à puce est d'utiliser la technologie RFID. Plusieurs milliards de dispositifs RFID sont vendues chaque année et aucun ingénieur ne doit ignorer cette technologie, ses fonctionnalités intéressantes, mais également ses failles de sécurité . Pour illustrer le cours, nous allons voir comment casser la sécurité d'une carte d'accès, d'un passeport biométrique, la manière de voler une voiture tout en étant 20000 km de là, etc. A partir de cette technologie, le cours décrit et généralise les principaux points auxquels il faut faire attention lors de la conception d'une application sécurisée. Développer à partir de zéro une solution sécurisée: -- Comment lire une norme. -- Mettre en oeuvre des outils cryptographiques. -- Envisager la solution dans son ensemble. -- ... Découvrir un nouveau domaine: l'informatique ubiquitaire, en particulier la RFID: -- Les applications de la vie quotidienne basées sur la RFID. -- Plusieurs milliards de dispositifs informatiques qui nous entourent. -- L'informatique, ce n'est plus uniquement des PC reliés entre eux. -- ...
Bibliographie :	Support obligatoire: copie des diapositives disponible sur le site icampus.

Autres infos :	INGI2347 vs INGI2144 -- INGI2347 est une introduction à la sécurité des réseaux et des applications informatiques. -- INGI2144 est un cours avancé sur la sécurité des applications. Préalables: -- Une connaissance générale des systèmes informatiques et de programmation est nécessaire. Les étudiants doivent avoir une formation générale en sécurité de l'information telle que fournie par INGI2347. -- Les étudiants qui ne savent pas si leur formation leur permet de suivre le cours (par exemple les étudiants ELEC, ELME ou MAP) doivent contacter le titulaire.
Cycle et année d'étude: :	> Master [120] en sciences informatiques > Master [120] : ingénieur civil en informatique > Master [120] : ingénieur civil électricien > Master [120] : ingénieur civil en mathématiques appliquées
Faculté ou entité en charge:	INFO