UCL Université catholique de Louvain

LINGI2144

2010-2011

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://www.icampus.ucl.ac.be/claroline/course/index.php?cid=INGI2144
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.
Thèmes abordés :	-- Introduction aux applications basées sur des jetons. -- RFID Primer: applications actuelles et les caractéristiques. -- Protocoles d'authentification, clé secrète et publique -- Exemples de mauvaises conceptions (MIT, DST), TMTO. -- Mise en place de blocs de la cryptographie. -- Implémentation de générateur de nombre pseudo-aléatoire. -- Exemples de mauvaises conceptions (Mifare). -- Attaques de relais et distance englobante. -- Confidentialité: fuites d'information et traçabilité malveillante. -- Déni de service. -- Etude de cas par un industriel. -- Cas du passeport biométrique.
Acquis d'apprentissage	L'objectif de ce cours est d'apprendre à construire une application sécurisée de la théorie à la pratique dans un environnement de production. Comme étude de cas, le cours se focalise sur les applications basées sur des jetons dont l'objectif principal est d'assurer l'authentification. Les étudiants ayant suivi avec succès ce cours seront capable de: -- concevoir de systèmes informatiques utilisant l'authentification par jeton en assurant la sécurité de ces systèmes -- implémenter une application sécurisée basée sur des jetons 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 -- évaluer la performance du système de sécurité mis en oeuvre. Les étudiants auront développé des compétences méthodologiques et opérationnelles. En particulier, ils auront développé leur capacité à -- rédiger un rapport technique succint permettant de mettre en lumière les principales caractéristiques d'un logiciel que l'on a développé, en utilisant à bonne escient la terminologie et les concepts théoriques, -- réaliser une démonstration probante d'un logiciel que l'on a développé, en choisissant les tests pertinents par rapport au cahier de charge et en s'assurant à l'avance que le logiciel les passe avec succès, -- 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 particulière 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 ne sont pas autorisés. 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 applcation sécurisée basée sur des jetons. -- 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 la matériel utilisé dans le cadre du projet.

Contenu :	La façon actuellement attractive pour effectuer une authentification avec jeton 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 omniprésente, 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 disponibles 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.
Cycle et année d'étude: :	> Master [120] : ingénieur civil en informatique > Master [120] en sciences informatiques > Master [120] : ingénieur civil en mathématiques appliquées > Master [120] : ingénieur civil électricien
Faculté ou entité en charge:	INFO