UCLouvain

lingi2144

2018

Secured systems engineering

5 crédits	30.0 h + 15.0 h	Q2

Enseignants	Legay Axel ;
Langue d'enseignement	Anglais
Lieu du cours	Louvain-la-Neuve
Thèmes abordés	L'objectif du cours est de sensibiliser l'étudiant au problème de la sécurité informatique en adoptant l'approche "ethical hacking" . L'approche suivie est celle qui consiste à montrer comment les vulnérabilités d'un système informatique peuvent être exploitées pour en menacer la sécurité. De là, l'étudiant développera les compétences nécessaires à la détection de ces vulnérabilités et aux mesures de protection du système. Ces dernières peuvent être déployées amont ou en aval (suivant le processus de développement). On s'intéressera aussi au coût et à la solidité de ces mesures. L'étudiant recevra aussi une très brève introduction à l'analyse de malware et aux techniques permettant de les détecter. Pendant ce cours, l'étudiant sera aussi sensibilisé à la place que prend la cyber sécurité en industrie, ainsi qu'aux problèmes éthiques qui sont liés à ce domaine. Pour information, les vulnérabilités abordées seront : buffer overflow, integer overflow, format string, data race. Parmi les protection on étudiera la technique de la pile non exécutable ou bien encore celle du « canary ». Pour l'analyse de malware, on s'intéressera à MIRAI et à l'outil YARA.
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: 1 • 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	**En première session:** • un examen qui compte pour 60% de la note finale • deux travaux qui comptent pour 40% de la note finale **En seconde session:** Un examen qui compte pour 100% de 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.
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. • ...
Ressources en ligne	https://moodleucl.uclouvain.be/enrol/index.php?id=12241
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 .
Faculté ou entité en charge:	INFO

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

Intitulé du programme	Sigle	Crédits	Prérequis	Acquis d'apprentissage
Master [120] : ingénieur civil en informatique	INFO2M	5		
Master [120] : ingénieur civil électricien	ELEC2M	5		
Master [120] en sciences informatiques	SINF2M	5		
Master [120] : ingénieur civil en mathématiques appliquées	MAP2M	5		