UCLouvain

linfo2144

2026

Secured systems engineering

5.00 crédits	30.0 h + 15.0 h	Q2

Langue d'enseignement	Anglais > Facilités pour suivre le cours en français
Lieu du cours	Louvain-la-Neuve
Préalables	Requis#: compétences en programmation dans le langage C telles qu'enseignées dans le cours LEPL1503 Requis#: principes des systèmes informatiques, tels que visés par le cours LINFO1252
Thèmes abordés	Ce cours introduit la sécurité des logiciels en explorant les fondements de la cybersécurité, les attaques logicielles et les vulnérabilités, comme celles qu'on peut trouver dans les protocoles cryptographiques, les cartes RFID et les passeports biométriques. Les étudiants examineront les techniques de protection contre les attaques et se familiariseront avec l'analyse des logiciels malveillants. Des sujets avancés incluent les dépassements d'entiers et de tampons, l'analyse statique et dynamique des malwares, ainsi que des exercices pratiques incluant la mise en place de pièges, l'analyse d'intrusions et de malwares.
Acquis d'apprentissage	**A la fin de cette unité d'enseignement, l'étudiant est capable de :** 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.
Modes d'évaluation des acquis des étudiants	Mode d'évaluation pour la **session de juin** : • Examen écrit (70% de la note finale) • Evaluation orale des travaux pratiques durant le quadrimestre (30% de la note finale) Mode d'évaluation pour la **session d'août** : • Examen écrit (100% de la note finale)
Méthodes d'enseignement	Cours magistraux, Lecture de littérature, Travaux pratiques
Contenu	Le cours propose une introduction à la sécurisation des systèmes informatiques au travers de divers thématiques. Exemples de sujets abordés les années précédentes:

	• Escalade et séparation de privilèges. • Sécurité mémoire (buffer overflow, stack overflow, exploits on dynamic memory allocations): attaques et contre-mesures; undefined behavior. • Analyse de malware statique et dynamique. • Conception de protocoles de communication sécurisés (exemple: TLS). • Systèmes d'authentification de machines: fondamentaux de cryptographie, certificats, TOFU... • Authentification d'utilisateurs: sécurité des mots de passe, authentification multi-facteurs, single sign-on (SSO). • Chaine d'approvisionnement logiciel: distribution sécurisée, mises à jour, dépendences, traçabilité. • Réponse à incident.
Ressources en ligne	https://moodle.uclouvain.be/course/view.php?id=3593
Bibliographie	Available on moodle. Disponible sur moodle.
Autres infos	INFO2144 vs INFO2347: • INFO2144 est un cours qui aborde plus en profondeur les thématiques ci-dessus. • INFO2347 est une introduction générale à la cybersécurité, avec une attention particulière à la sécurité des réseaux et des applications web. Préalable(s): • Une connaissance générale des systèmes informatiques et de programmation est nécessaire. Suivre le cours INFO2347 n'est pas nécessaire pour aborder le cours INFO2144.
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 électricien	ELEC2M	5		
Master [120] : ingénieur civil en informatique	INFO2M	5		
Master [120] en sciences informatiques	SINF2M	5		
Master [120] : ingénieur civil en mathématiques appliquées	MAP2M	5		
Master [120] : ingénieur civil en science des données	DATE2M	5		
Master [120] en science des données, orientation technologies de l'information	DATI2M	5		