UCLouvain

lingi2144

2020

Secured systems engineering

En raison de la crise du COVID-19, les informations ci-dessous sont susceptibles d'être modifiées, notamment celles qui concernent le mode d'enseignement (en présentiel, en distanciel ou sous un format comodal ou hybride).

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 de ce cours est de maîtriser les bases de la sécurité logiciel. Au travers d'exemples concrets, on apprendra à détecter les erreurs de programmation pouvant mener à des exploits (hack) informatique. Ensuite, on étudiera des méthodes pour se prémunir de ces exploits. Le coûts et les limites de ces méthodes de prévention seront évaluées. Pour finir, une introduction à la virologie informatique sera donnée.
Acquis d'apprentissage	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 étudiant.es ayant suivi avec succès ce cours seront sensibilité à la cyber sécurité et à la protection du système d'informations. Elles/ils seront capables de: 1 • Comprendre les dangers et les effets d'une attaque cyber ; • concevoir de programmes informatiques sécurisés ; • détecter des vulnérabilités logiciels et les corriger. Les étudiants auront donc développé des compétences méthodologiques et opérationnelles. En particulier, ils auront développé leur capacité à • rédiger un rapport technique succinct 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 ; - - - - *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 raison de la crise du COVID-19, les informations de cette rubrique sont particulièrement susceptibles d'être modifiées.** **En première session:** Un examen oral pour ceux qui le désirent, sinon on prend la somme des points des deux travaux. **En seconde session:** Un examen qui compte pour 100% de la note finale.
Méthodes d'enseignement	**En raison de la crise du COVID-19, les informations de cette rubrique sont particulièrement susceptibles d'être modifiées.** Cours théoriques et travaux pratiques. Intervenants extérieurs pour présenter des problèmes d'actualité.
Contenu	L'objectif du cours est de donner une introduction à la sécurité logiciel. Dans un premier temps, on abordera les conceptes de sécurité et d'attaque logiciel. Nous analyserons ensuite des vulnérabilités logiciel et nous étudierons des protections. Pour terminer, une introduction à l'analyse de malwares sera présentée. Contenu. - Introduction à la cyber sécurité - Introduction aux notions de vulnérabilités, menaces et attaques - Introduction au fishing

	- Introduction à l'escalade de privilège - Integer overflow - Buffer overflow: assembleur, protection et contre attaque - Format string et vulnérabilités du langage C - Ecriture de "shellcode" - Introduction aux analyses statiques et dynamiques de malwares - Honey pots - Analyse dynamique de mémoire - Packing et cracking - Intervenants extérieurs: la sécurité à l'UCLouvain, chez CISCO et chez NVISO. - Exercices pratiques sur ordinateurs - Travaux pratiques: mise en place de pièges, intrusion, analyse de malware
Ressources en ligne	https://moodleucl.uclouvain.be/enrol/index.php?id=12241
Bibliographie	Available on moodle. Disponible sur moodle.
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. Suivre le cours INGI2347 n'est pas nécessaire pour aborder le cours INGI2144. • 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.
Faculté ou entité en charge:	INFO

Force majeure

Modes d'évaluation des acquis des étudiants	En première session: Les étudiant.es qui le désirent peuvent garder les points de leurs travaux. Elles/Ils ont aussi la possibilité de présenter un examen oral sur l'ensemble de la matière. Dans ce dernier cas, les travaux comptent pour 40% et l'examen oral pour 60%. En seconde session: un examen oral (théorique et pratique) sur l'ensemble de la matière.

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] en sciences informatiques	SINF2M	5		
Master [120] : ingénieur civil électricien	ELEC2M	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		