






Au vu du contexte sanitaire lié à la propagation du coronavirus, les modalités d'organisation et d'évaluation des unités d'enseignement ont pu, dans différentes situations, être adaptées ; ces éventuelles nouvelles modalités ont été -ou seront- communiquées par les enseignant-es aux étudiant-es.

5 crédits	30.0 h + 15.0 h	Q2
-----------	-----------------	----

Enseignants	Legay Axel ;
Langue d'enseignement	Anglais
Lieu du cours	Louvain-la-Neuve
Thèmes abordés	<p>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.</p> <ul style="list-style-type: none"> • Introduction à la cyber sécurité et la virologie • Vulnérabilités exploitables par menaces et attaque • Vulnérabilités du langage C (Buffer overflow, heap, format string) et protections • Shell code : écriture en C/assembleur • Classification de malwares • Détection de malwares • Techniques statiques, dynamiques et par intelligence artificielle.
Acquis d'apprentissage	<p>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 :</p> <ul style="list-style-type: none"> • INFO1.1-3 • INFO2.1-5 • INFO5.2, INFO5.4-5 • INFO6.1, INFO6.3, INFO6.4 <p>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 :</p> <ul style="list-style-type: none"> • SINF1.M1 • SINF2.1-5 • SINF5.2, SINF5.4-5 • SINF6.1, SINF6.3, SINF6.4 <p>1</p> <p>Les étudiants ayant suivi avec succès ce cours seront capables de:</p> <ul style="list-style-type: none"> • concevoir des systèmes informatiques sécurisés • implémenter une application sécurisée basée et tester la sécurité d'applications existantes • expliciter les techniques et outils utilisé en matière de sécurité afin de convaincre les utilisateurs potentiels que ces aspects ont correctement été pris en compte. <p>Les étudiants auront développé des compétences méthodologiques et opérationnelles. En particulier, ils auront développé leur capacité à</p> <ul style="list-style-type: none"> • prendre en compte les dimensions éthiques 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. <p>----</p> <p><i>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) ».</i></p>
Modes d'évaluation des acquis des étudiants	<p>En raison de la crise du COVID-19, les informations de cette rubrique sont particulièrement susceptibles d'être modifiées.</p> <p>En première session:</p> <ul style="list-style-type: none"> • un examen qui compte pour 60% de la note finale • deux travaux qui comptent pour 40% de la note finale <p>En seconde session: Un examen qui compte pour 100% de la note finale.</p>

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 concepts 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 <ul style="list-style-type: none"> • INGI2347 est une introduction à la sécurité des réseaux et des applications informatiques. • INGI2144 est un cours avancé sur la sécurité des applications. Préalables: <ul style="list-style-type: none"> • 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

Programmes / formations proposant cette unité d'enseignement (UE)				
Intitulé du programme	Sigle	Crédits	Prérequis	Acquis d'apprentissage
Master [120] : ingénieur civil en science des données	DATE2M	5		
Master [120] : ingénieur civil en informatique	INFO2M	5		
Master [120] : ingénieur civil en mathématiques appliquées	MAP2M	5		
Master [120] en sciences informatiques	SINF2M	5		
Master [120] : ingénieur civil électricien	ELEC2M	5		
Master [120] en science des données, orientation technologies de l'information	DATI2M	5		