javaUniversité du Québec en Outaouais **Département d'informatique et d'ingénierie**

Sigle : CYB1173 Gr. 01
Titre : Sécurité du logiciel
Session : Hiver 2025 **Horaire et local**
Professeur : Khoury, Raphaël

1. Description du cours paraissant à l'annuaire :

Objectifs
Au terme de ce cours, l'étudiant.e aura une compréhension de la problématique et des solutions pour la construction et l'évaluation de logiciels fiables dans des environnements possiblement hostiles.

Contenu

Vulnérabilités et faiblesses des logiciels, leur identification et gestion. Principes de conception de logiciels sécuritaires dans un environnement hostile. Attaques et robustesse contre les attaques. Gestion de la mémoire et vérification des limites. Sécurité par conception dans toutes les phases de développement, des besoins au code. Choix et utilisation de composantes fiables, identification et bonification de code faible ou vulnérable. Méthodes formelles, analyse formelle et vérification formelle de propriétés de sécurité. Méthodes de test de propriétés de sécurité. Ce cours comporte des séances obligatoires de travaux pratiques (TP).

Descriptif - Annuaire

2. Objectifs spécifiques du cours :

- L'objet du cours est de familiariser l'étudiant avec la sécurité logicielle, c'est-à-dire l'ensemble des théories, des pratiques, des vérifications et des prudences que devraient utiliser les programmeurs afin que les systèmes qu'ils développent soient aussi sécuritaires que possible.

3. Stratégies pédagogiques :

- Cours magistraux donnés en mode présentiel
- Le cours sera accompagné de lectures obligatoires
- Conformément aux règlements de l'UQO, jusqu'à 3 séances pourraient être donné en mode non-présentiel.
- Devoirs
- Examen de mi-session (présentiel)
- Examen final (présentiel)

4. Heures de disponibilité ou modalités pour rendez-vous :

Heures de consultation : Sur rendez-vous.
Bureau : B-2020

Email : raphael.khoury@uqo.ca

5. Plan détaillé du cours sur 15 semaines :

Semaine	Thèmes	Dates
1	**Notions de base et Les 8 principes de Saltzer et Schroeder** • La triade CID (Intégrité, Confidentialité et Disponibilité) • Les principes de base de la sécurité de l'information	14 janvier 2025
2	**Le dépassement de tampon (buffer overflow)** • Structure de la pile d'appel • Causes dépassement de tampon et contremesures Exemples réels	21 janvier 2025
3	**La sécurité des entiers**	28 janvier 2025

	• Les différents types d'entiers Les causes et mécanismes de défenses contre l'overflow d'entier Présentation du Devoir 1 : Les principes.	
4	**Le subterfuge de pointeur et la corruption de la mémoire** • Causes et conséquences • Exemples réels	4 février 2025
5	**La Génération des nombres aléatoires** • Les PRNG et les TRNG • Les algorithmes pour tester les nombres aléatoires Devoir 2 : Les nombres aléatoires	11 février 2025
6	**La vulnérabilité de traverse de répertoire et Protéger les secrets** • Cause de la vulnérabilité de traverse de répertoire • La canonisation • Le ransomware Locky • Autres vulnérabilités de la gestion des fichiers	18 février 2025
7	**Sécurité des Bases de données et Injection SQL** • Chiffrement des BD • Sauvegarde et protection des données • L'injection SQL : fonctionnement et mécanisme de défense • Études de cas	25 février 2025
8	**Semaine de relâche**	3 au 7 mars 2025
9	**Examen 1**	11 mars 2025
10	**Les optimisations dangereuses** • Les optimisations effectuées par les compilateurs • Les contremesures Mini Devoir 1 : Les optimisations	18 mars 2025
11	**La sécurité des fichiers et les erreurs cryptographiques et l'attaque Redos** • Les types d'erreurs cryptographiques • L'attaque Redos Mini devoir 2 : L'attaque redos	25 mars 2025
12	**La sécurité de Java** • Les fonctionnalités de sécurité de Java • L'attaque de désérialisation Devoir 3 : L'attaque de désérialisation	1 avril 2025
13	**Le contrôle d'accès et la sécurité de l'OS** • La sécurité sur Windows • La sécurité sur Linux • Étude de cas : le Rootkit Sony	8 avril 2025
14	**À déterminer**	15 avril 2025
15	**Examen final (3h)**	22 avril 2025

6. Évaluation du cours :

- Examen de mi-session : 25 %
- Examen final : 25 %
- Devoir 1 (principes): 15%
- Devoir 2 (les nombres aléatoires): 15%
- Devoir 3 (la désérialisation) : 15%
- Mini devoirs 1 et 2 (combiné) : 5%

7. Politiques départementales et institutionnelles :

- Politique du département d'informatique et d'ingénierie relative à la tenue des examens
- Note sur le plagiat et sur la fraude
- Politique relative à la qualité de l'expression française écrite chez les étudiants et les étudiantes de premier cycle à l'UQO
- Absence aux examens : cadre de gestion, demande de reprise d'examen (formulaire)

Tolérance ZÉRO en matière de violence à caractère sexuel.

Le Bureau d'intervention et de prévention en matière de harcèlement (BIPH) a pour mission d'accueillir, soutenir et guider toute personne vivant une situation de harcèlement, de discrimination ou de violence à caractère sexuel. Le BIPH oriente ses actions afin de prévenir les violences à caractère sexuel pour que nous puissions étudier, travailler et s'épanouir dans un milieu sain et sécuritaire.
Vous vivez ou êtes une personne témoin d'une situation de violence à caractère sexuel ? Vous êtes une personne membre de la communauté étudiante ou une personne membre du personnel, autant à Gatineau qu'à Ripon et St-Jérôme, l'équipe du BIPH est là pour vous, sans jugement et en toute confidentialité.
Ensemble, participons à une culture de respect.
Pour de plus amples renseignements consultez UQO.ca/biph ou écrivez-nous au Biph@uqo.ca

8. Principales références :

Référence Principale :

- Raphaël Khoury, La Sécurité logicielle : une approche défensive, Presses de l'université Laval, 2023.

Autres références :

- Robert Seacord, Secure Coding in C and C++, Addison-Wesley Professional, 2nd edition.
- Charles P. Pfleeger, Shari Lawrence Pfleeger, Jonathan Margulies, Security in Computing, 5e edition, Pearson, 2015
- William Stallings, Lawrie Brown, Computer Security: Principles and Practice, 3e edition, Pearson 2015

9. Page Web du cours :

https://moodle.uqo.ca