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

Sigle : CYB1133 Gr. 20
Titre : Sécurité des données et contrôle d'accès au niveau organisationnel
Session : Hiver 2026 **Horaire et local**
Professeure : Bouhaddi, Myria

1. Description du cours paraissant à l'annuaire :

Objectifs
Permettre aux étudiants de maîtriser les aspects informatiques de la conception et implémentation de méthodes de protection et contrôle d'accès aux données dans les entreprises, du point de vue des exigences d'entreprise, de la structure des logiciels, de la validation des exigences et de la conception de systèmes.

Contenu

Exigences de sécurité des données et de protection de la vie privée. Politiques de protection et contrôle d'accès d'entreprise. Méthodes de contrôle d'accès discrétionnaires et non-discrétionnaires, caractéristiques logiques et implémentation. Rôles d'entreprise. Conception de rôles. Contrôle d'accès basé sur les rôles (RBAC) et ses variantes. Contrôle d'accès basé sur les attributs. Méthodes Bell-LaPadula, Biba et muraille de Chine. Modèles hybrides. Langages pour la spécification d'exigences et de politiques de contrôle d'accès. Principes et méthodes pour l'analyse du risque dans le contrôle d'accès. Étude de la littérature et d'outils courants.

Descriptif – Annuaire

2. Objectifs spécifiques du cours :

À terme, l'étudiant (e) sera au fait des problématiques liées au domaine du contrôle d'accès aux données et sera capable de maîtriser le processus de développement de ces systèmes dans des contextes d'entreprise en utilisant des outils industriels et des techniques formelles de spécification et de validation. Il ou elle sera capable d'évaluer différentes solutions pour les problèmes de protection d'accès et de protection de la vie privée dans des contextes d'entreprise.

3. Stratégies pédagogiques :

Cours majoritairement magistral, mais encourageant une participation active des étudiants avec interventions et présentations. Donné à distance avec examens administrés par internet.

Les étudiant(e)s qui s'inscrivent à ce cours doivent s'assurer qu'ils ont :

- un ordinateur (avec un système d'exploitation Windows);
- une connexion Internet;
- une webcam;
- un microphone;
- la suite Office 365 (les étudiant(e)s ont un accès gratuit à la suite Office 365 : https://uqo.ca/sti/outils-numeriques).

Guide d'utilisation de Zoom à l'intention des étudiants

Soutien à l'apprentissage et à la réussite | Université du Québec en Outaouais

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

Communication par courriel (myria.bouhaddi@uqo.ca) et via le forum de discussion. Rencontres sur Zoom.

5. Plan détaillé du cours sur 15 semaines :

Semaine	Thèmes	Dates
1	**Introduction à la sécurité des données et au contrôle d'accès** • Enjeux de la sécurité des données en entreprise • Notions de base du contrôle d'accès • Historique des systèmes de contrôle d'accès • Rôle stratégique des contrôles d'accès dans la cybersécurité organisationnelle. • Exemples concrets d'incidents liés à des contrôles d'accès inadéquats	13 jan. 2026
2	**Gestion des identités et authentification** • Identification vs authentification vs autorisation • Facteurs d'authentification : mots de passe, biométrie, tokens, etc.	20 jan. 2026

	• Authentification multifactorielle (MFA) : concept, outils et implémentation • Vulnérabilités et attaques sur l'authentification • Étude de cas : analyse critique d'une solution MFA dans une entreprise	
3	**Contrôle d'accès centralisé basé sur un annuaire** • Principes de la gestion centralisée des identités • Rôle des annuaires dans les systèmes d'information • Introduction à Active Directory. : utilisateurs, groupes et unités organisationnelles • Lien entre identités, groupes et droits d'accès **Travail dirigé 1 : 30 janvier 2026**	27 jan. 2026
4	**Contrôles d'accès discrétionnaires (DAC)** • Principe des contrôles DAC • Permissions sous Linux/Unix • Matrices de contrôle d'accès : conception et limites • Forces et faiblesses du modèle DAC en entreprise • Atelier pratique : configuration de permissions sous Linux. **Travail dirigé 2 : 06 février 2026** **Devoir 1**	03 fév. 2026
5	**Contrôles d'accès obligatoires (MAC)** • Classification des données et niveaux de sensibilité • Modèles Bell–LaPadula et Biba • Contextes d'application (gouvernement, défense) • Limites des MAC dans les environnements modernes • Étude de cas : mise en œuvre des politiques MAC dans un contexte gouvernemental **Travail dirigé 3 : 13 février 2026**	10 fév. 2026
6	**Contrôles d'accès basés sur les rôles (RBAC)** • Concepts et principes du RBAC • RBAC classique et variantes • Principe de moindre privilège • Séparation des tâches • Implémentation du RBAC dans les systèmes réels (applications, Active Directory) **Travail dirigé 4 : 20 février 2026**	17 fév. 2026
7	**Contrôles d'accès basés sur les attributs (ABAC)** • Principes du contrôle d'accès basé sur les attributs • Attributs utilisateur, ressource et contexte • Politiques dynamiques et décisions contextuelles • Comparaison RBAC vs ABAC • Étude de cas : simulation de scénarios ABAC en entreprise. **Travail dirigé 5 : 27 février 2026**	24 fév. 2026
8	**Semaine d'études**	03 mar. 2026
9	**Examen de mi-session**	10 mar. 2026
10	**Extraction de rôles et ingénierie des rôles** • Problèmes liés à la conception et à l'évolution des rôles • Méthodes d'extraction et d'ingénierie des rôles • Optimisation et gestion continue des rôles **Travail dirigé 6 : 20 mars 2026** **Devoir 2** **Projet de session**	17 mar. 2026
11	**Mécanismes de surveillance et audit**	24 mar. 2026

	• Concepts de traçabilité et de non-répudiation • Journaux d'accès (Linux et Windows) • Introduction aux SIEM • Enjeux de l'anonymat et de la protection de l'identité Atelier : configuration de journaux d'audit pour un système.	
12	**Évaluation des stratégies et analyse des risques** • Impact des contrôles d'accès sur la sécurité globale • Évaluation de l'efficacité d'une stratégie de contrôle d'accès • Analyse des risques liés aux permissions excessives • Utilisation des journaux pour l'évaluation et la prise de décision **Travail dirigé 7 : 03 avril 2026**	31 mar. 2026
13	**Techniques modernes d'authentification et de contrôle d'accès technique** • Stockage sécurisé des mots de passe • Hachage, salage et bonnes pratiques • MFA avancé : TOTP, biométrie, SMS • Sécurité des jetons d'accès. **Travail dirigé 8 : 10 avril 2026**	07 avr. 2026
14	**Présentation des projets** Exercices de révision	14 avr. 2026
15	**Examen final**	21 avr. 2026

6. Évaluation du cours :

- Devoir 1 : 10 %
- Devoir 2 : 10 %
- Projet de session : 25 %
- Examen de mi-session : 25 %
- Examen final: 30 %

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 :

1. D.F. Ferraiolo, D.R. Kuhn, R. Chandramouli: Role-Based Access Control. 2nd edition, Artech House, 2007 (copie papier et accès en ligne dans la bibliothèque).
2.V.C. Hu, D.F. Ferraiolo, R. Chandramouli, D.R. Kuhn : Attribute-Based Access Control. Artech House, 2018 (copie papier et accès en ligne dans la bibliothèque).

9. Page Web du cours :

https://moodle.uqo.ca