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

Sigle : CYB1133 Gr. 01
Titre : Sécurité des données et contrôle d'accès au niveau organisationnel
Session : Hiver 2025 Horaire et local
Professeur : Bouhaddi, Myria

1. Description du cours paraissant à l'annuaire :

Objectifs

Au terme de ce cours, l'étudiant.e aura acquis une compréhension de la problématique et des solutions pour la protection de données dans les organisations, comme le gouvernement, les banques et le militaire, ainsi qu'une compréhension des modèles abstraits et outils existants à cette fin.

Contenu

Principes généraux et besoins. Secret, confidentialité, intégrité, disponibilité. Besoin de savoir, moindre privilège, conflits d'intérêt, vie privée. Politiques, modèles et administrations. Contrôle d'accès et contrôle de flux de données. Domaines, sessions et flux de travaux. Mise en œuvre de la sécurité des données dans les systèmes d'exploitation. Canaux cachés. Modèles de contrôle d'accès principaux, tels que: matrices de contrôle d'accès, contrôle d'accès discrétionnaire, contrôle d'accès obligatoire, contrôle d'accès basé sur les rôles, contrôle d'accès basé sur les attributs. Windows Active Directory et SE-Linux. Avantages et limitations de chaque modèle, autres modèles pertinents. Vérifications (audits). Ce cours comporte des séances obligatoires de travaux dirigés (TD).

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

Site pour soutien de réussite en mode non-présentiel : uqo.ca/etudier-non-presentiel.

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 au contrôle d'accès et contexte organisationnel** • Notions de base • 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.	15 janvier 2025

2	**Identification et authentification** • Introduction aux mécanismes d'identification et d'authentification. • Facteurs d'authentification : mots de passe, biométrie, tokens, etc. • Authentification multifactorielle (MFA) : concept, outils et implémentation. • Étude de cas : analyse critique d'une solution MFA dans une entreprise. **Travail pratique 1 : 21 janvier 2025**	22 janvier 2025
3	**Contrôles d'accès discrétionnaires (DAC)** • Permissions ponctuelles et structures de contrôle DAC. • Analyse du modèle UNIX-Linux : forces et limites. • Matrices de contrôle d'accès : conception et analyse. • Atelier pratique : configuration de permissions sous Linux. **Travail pratique 2 : 28 janvier 2025** **Devoir 1**	29 janvier 2025
4	**Contrôles d'accès basés sur les attributs (ABAC)** • Introduction au contrôle d'accès basé sur les attributs. • Politiques de sécurité et critères d'accès contextuels. • Étude des attributs dynamiques. • Étude de cas : simulation de scénarios ABAC en entreprise. **Travail pratique 3 : 4 février 2025**	5 février 2025
5	**Contrôles d'accès basés sur les rôles (RBAC)** • Concept et mise en œuvre des rôles. • RBAC classique et variantes modernes. • Séparation des tâches et principe de moindre privilège. • Séparation des tâches • Atelier : conception d'une politique RBAC pour une entreprise fictive. **Travail pratique 4 : 11 février 2025**	12 février 2025
6	**Contrôles d'accès obligatoires (MAC)** • Niveaux de sensibilité et classification des données. • Modèles Bell-LaPadula et Biba : principes et applications. • Limites des contrôles MAC dans les environnements modernes. • Étude de cas : mise en œuvre des politiques MAC dans un contexte gouvernemental. **Travail pratique 5 : 18 février 2025** **Devoir 2**	19 février 2025
7	**Mécanismes avancés de surveillance et audit** • Concept de non-répudiation et traçabilité. • Outils de surveillance : journaux d'accès, SIEM (Security Information and Event Management). • Anonymat et protection de l'identité. • Atelier : configuration de journaux d'audit pour un système.	26 février 2025
8	**Semaine d'études**	5 mars 2025
9	**Examen de mi-session**	12 mars 2025
10	**Modèles hybrides et stratégies avancées** • Modèle Brewer and Nash (Muraille de Chine). • Contrôle d'accès basé sur le contexte (Context-Aware Access Control). • Stratégies d'implémentation dans des environnements cloud et hybrides. **Travail pratique 6 : 18 mars 2025** **Projet de session :** système de gestion des accès basé sur un serveur web avec authentification adaptative et audit des activités	19 mars 2025

11	**Outils de spécification des politiques de contrôle d'accès** • Langages de spécification (XACML, ALFA). • Centralisation des accès et privilèges : implémentation et enjeux. • Étude de cas : mise en place d'une politique centralisée pour un système complexe. **Travail pratique 7 : 25 mars 2025**	26 mars 2025
12	**Techniques modernes d'authentification et de contrôle d'accès technique** • Obfuscation des mots de passe et outils modernes de hachage. • Implémentation d'authentification à facteurs multiples (MFA) : SMS, TOTP, biométrie. • Étude de la sécurité des jetons d'accès. • Atelier pratique : implémentation d'un système MFA. **Travail pratique 8 : 1 avril 2025**	2 avril 2025
13	**Évaluation des stratégies et analyse des risques** • Impact des contrôles d'accès sur la sécurité globale. • Méthodes d'analyse des risques liés aux accès non autorisés. • Étude de l'impact sur la protection des données personnelles (RGPD, HIPAA). • Atelier : analyse critique d'une stratégie existante.	9 avril 2025
14	**Principes d'analyse et tendances futures** • Contrôles d'accès dans les environnements IoT et cloud. • Intelligence artificielle et machine learning pour la gestion des accès. • Sécurité des API et intégrations avec des systèmes tiers. • Atelier : simulation de menaces dans un environnement IoT.	16 avril 2025
15	**Examen final**	23 avril 2025

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