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

Sigle : CYB6053 Gr. 01
Titre : Sécurité des systèmes embarqués et de l'internet des objets
Session : Automne 2025 **Horaire et local**
Professeur : Abderrahmane Ben Mimoune

1. Description du cours paraissant à l'annuaire :

Objectifs
Au terme de ce cours, l'étudiant.e sera en mesure de réaliser une analyse poussée sur menaces et des vulnérabilités associées aux systèmes embarqués et connectés dans l'internet des objets et de préserver la sécurité des applications, des données et des protocoles de communication.

Contenu
Introduction aux systèmes embarquées et aux architectures des systèmes dans l'internet des objets. Technologies les plus utilisées et les principales plateformes pour l'internet des objets. Vulnérabilités et menaces spécifiques aux systèmes embarqués dans l'internet des objets. Mécanismes d'authentification décentralisés. Sécurité dans les réseaux Ad-hoc : partage de secret, certification, etc. Sécurité des protocoles de communication : norme zigbee, etc. Études de cas : domotique, villes intelligentes, etc.

Descriptif - Annuaire

2. Objectifs spécifiques du cours :

À la fin de ce cours, l'étudiant.e devrait être en mesure de:

- Expliquer les fondements des systèmes embarqués et de l'architecture de l'internet des objets.
- Identifier et caractériser les principales vulnérabilités et menaces affectant les objets connectés.
- Analyser les risques de sécurité associés aux applications, données et protocoles dans les services IoT.
- Mettre en œuvre des mécanismes de sécurité décentralisés.
- Concevoir et évaluer des solutions de sécurité pour les environnements IoT.
- Adopter une démarche critique pour intégrer la sécurité dès la phase de conception des systèmes embarqués.

3. Stratégies pédagogiques :

- Cours magistraux : 3 h/semaine de cours
- Un devoir
- Un projet de session
- Un examen de mi-session
- Un examen final

Disponibilité d'une page MOODLE contenant le matériel du cours et les résultats des évaluations.

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

- Disponible pour répondre aux courriels dans un délai typique de 72 heures.
- Disponible durant les séances du cours pour répondre aux questions.
- Pour obtenir un rendez-vous, envoyez un courriel à : Abderrahmane.BenMimoune@uqo.ca

5. Plan détaillé du cours sur 15 semaines :

Semaine	Thèmes	Dates
1	**Cours 1** : Présentation du plan de cours, des activités évaluées, Introduction, définitions clés et cas d'usage	05 sept. 2025
2	**Cours 2:** Modèles d'architecture IoT: Vue d'ensemble, niveaux de vulnérabilités dans l'architecture, les couches architecturales de l'IoT, standards d'architecture	12 sept. 2025 **(non présentiel)**
3	**Cours 3:** La réseautique dans IoT, les protocoles de communication et applicatifs IoT, sécurisation des protocoles de communication	19 sept. 2025
4	Férié – Jour de la vérité et de la réconciliation	26 sept. 2025
5	**Cours 4:** Sécurité dans les réseaux distribués et ad-hoc, l'infonuagiques et les enjeux liés à la gestion serveur/cloud dans l'IoT	03 oct. 2025
6	**Cours 5:** Les services infonuagiques et gestion des identités et des accès	10 oct. 2025
7	**Semaine d'études**	13-17 oct. 2025
8	**Examen de mi-session**	24 oct. 2025
9	**Cours 6:** Résilience, détection d'intrusions, surveillance, redondance et tolérance aux pannes	31 oct. 2025
10	**Cours 7:** Protection et confidentialité des données IoT, cycle de vie des données	07 nov. 2025
11	**Cours 8:** Sécurité des applications IoT : mobile/web. Meilleures pratiques : OWASP Top 10 Mobile + IoT	14 nov. 2025 **(non présentiel)**
12	**Cours 9:** Études de cas 1	21 nov. 2025
13	**Cours 10:** Études de cas 2	28 nov. 2025 **(non présentiel)**
14	**Présentation des projets**	05 déc. 2025
15	**Examen final**	12 déc. 2025

6. Évaluation du cours :

L'évaluation du cours se fera comme suit :

- Devoir : 15 %
- Projet : 25 %
- Examen de mi-session : 25 %
- Examen final : 35 %

Disponibilité d'une page MOODLE contenant le matériel du cours et les résultats des évaluations.

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 :

- Les réseaux - L'ère des réseaux cloud et de la 5G, Eyrolles, 2018.
- Demystifying Internet of Things Security, Apress Open, 2020
- Practical Internet of Thing Security, Packt Publishing Ltd, 2016
- A Beginner's Guide to Internet of Things Security: Attacks, Applications, Authentication, and Fundamentals, CRC Press, 2020

9. Page Web du cours :

https://moodle.uqo.ca