

Sigle : CYB6053 Gr. 01**Titre : Sécurité des systèmes embarqués et de l'internet des objets****Session : Automne 2026 Horaire et local****Professeur : Dr. Dhaou Said****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 embarqués 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 : dhaou.said@uqo.ca

5. Plan détaillé du cours sur 15 semaines :

Semaine	Thèmes	Dates
1	Cours 0 : Présentation du plan de cours, des activités évaluées, Introduction, définitions clés et cas d'usage	09 sept. 2026
2	Cours 1: Modèles d'architecture IoT : Vue d'ensemble, les couches architecturales de l'IoT, standards d'architecture	16 sept. 2026
3	Cours 2: La Réseautique & les Protocoles de Communication IoT & Sécurité Partie 1 : Réseaux et Protocoles IoT de communication; Défis d'interconnexion, réseaux d'accès LPWAN et architectures applicatives MQTT & CoAP; Partie 2 : Sécurisation des protocoles de communication et les enjeux liés à la gestion des architectures IoT; Sécurité des systèmes embarqués et de IoT; Partie 3 : Sécurité au niveau du processeur et du matériel;	23 sept. 2026
4	Cours 3: Protection et Confidentialité des Données IoT - Le Cycle de Vie des Données TinyML : L'Intelligence Artificielle Ultra-Basse Consommation Présentations des projets	30 sept. 2026
5	Cours 5: Architecture Matérielle & Racine de Confiance Partie 1 : Root of Trust (RoT) & Démarrage sécurisé ; Partie 2 : Micro-logiciels (Firmware) & Attaques logicielles	07 oct. 2026
6	Semaine d'études	14 oct. 2026
7	Cours 6 : Études de cas 1 (devoir)	21 oct. 2026
8	Examen de mi-session	28 oct. 2026
9	Cours 7: Les services infonuagiques IoT et leurs applications dans une architecture IoT • Protocole, Cryptographie & Réseau IoT • Cryptographie légère & Transition Post-Quantique (PQC)	04 nov. 2026
10	Cours 8 : Études de cas 2 (devoir)	11 nov. 2026
11	Cours 9: Résilience, détection d'intrusions, surveillance des systèmes IoT • Sécurité des réseaux locaux & Périphériques sans fil	18 nov. 2026
12	Cours 10: Redondance et tolérance aux pannes dans les systèmes IoT • Réseaux étendus à faible puissance (LPWAN)	25 nov. 2026
13	Cours 11: Attaques Physiques, Canaux Auxiliaires & Analyse Avancée : • Interfaces de débogage et d'interconnexion • Attaques par canal auxiliaire (Side-Channel Attacks - SCA) • Injection de fautes (Fault Injection Attacks) • Mises à jour sécurisées (OTA - Over-The-Air) • DevSecOps embarqué, SBOM & Gestion des vulnérabilités • L'IA dans la sécurité IoT	02 déc. 2026
14	Présentation des projets	09 déc. 2026
15	Examen final	16 déc. 2026

6. Évaluation du cours :

L'évaluation du cours se fera comme suit :

- Devoir : 10 %
- Projet : 30 %
- 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](https://uqo.ca/biph) ou écrivez-nous au Biph@uqo.ca

8. Principales références :

- [1] Building Secure Cars / IoT Devices – Axelle Apvrille & al.
- [2] Hardware Hacking Handbook – Jasper van Woudenberg & Colin O'Flynn (No Starch Press).
- [3] Designing Secure IoT Devices – Brian Russell & Drew Van Duren.
- [4] Documentation & Normes : NIST SP 800-213, ETSI EN 303 645, ISO/IEC 27400.
- [5] Les réseaux - L'ère des réseaux cloud et de la 5G, Eyrolles, 2018.
- [6] Demystifying Internet of Things Security, Apress Open, 2020.
- [7] Practical Internet of Thing Security, Packt Publishing Ltd, 2016.
- [8] 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>