Programme court de deuxième cycle en cybersécurité - 0935

RESPONSABLE :

Gatineau

Pour de plus amples informations :

Téléphone : 819 595-3900, poste 1614
Courriel : csinfo@uqo.ca

SCOLARITÉ :

12 crédits, Deuxième cycle

OBJECTIFS :

Ce programme s'adresse à des professionnels ou des personnes qui veulent parfaire leurs connaissances dans les différents aspects de la cybersécurité. Il vise à les former sur des sujets de pointe dans ce domaine. Au terme de ce programme, les étudiants auront une connaissance approfondie des enjeux, des besoins et des solutions techniques en sécurité des réseaux et systèmes informatiques. Ils auront acquis une formation spécialisée pour mieux comprendre les technologies avancées en cybersécurité afin de les utiliser dans leur environnement de travail.

INFORMATIONS SUR L'ADMISSION :

Lieu d'enseignement	Régime	Trimestres d'admission		
		Automne	Hiver	Été
Gatineau	TP	✓	✓	

TP : Temps partiel

CONDITIONS D'ADMISSION :

Base études universitaires

Être titulaire d'un baccalauréat en informatique, en génie informatique, en génie électrique ou dans un domaine connexe (ex. mathématiques, sciences des systèmes), obtenu avec une moyenne cumulative d'au moins 3,2 (sur 4,3) ou l'équivalent.

Tout dossier de candidature avec une moyenne inférieure à 3,2 mais supérieure à 2,8 sur 4,3 sera étudié par le sous-comité d'admission et d'évaluation du programme et pourrait, dans certains cas, faire l'objet d'une recommandation d'admission.

Les dossiers de candidats détenteurs d'un baccalauréat obtenu avec une moyenne cumulative inférieure à 2,8 sur 4,3, mais égale ou supérieure à 2,5 sur 4,3 (ou l'équivalent) seront étudiés par le sous comité d'admission et d'évaluation, à la condition de posséder une formation additionnelle et appropriée d'au moins 15 crédits universitaires (ou l'équivalent) complétés avec une moyenne cumulative d'au moins 3,2 sur 4,3 (ou l'équivalent). Ils pourront faire, dans certains cas, l'objet d'une recommandation d'admission.

Le comité d'admission du programme se réserve le droit d'imposer des cours d'appoint (de 1 à 9 crédits) ou un programme de propédeutique (de 10 à 30 crédits) au candidat qui ne répond pas entièrement aux conditions d'admission du programme.

Base expérience

Le candidat n'ayant pas fait d'études universitaires, mais qui a complété des études collégiales, pourra être admis à un programme de deuxième cycle s'il a au moins douze années d'expérience de travail à la fois pertinente et significative, eu égard à la discipline ou au champ d'études du programme pour lequel il sollicite l'admission.

Dans le cas du candidat qui, sans avoir complété un baccalauréat, a néanmoins obtenu des crédits universitaires, le nombre d'années d'expérience requis sera modulé en fonction des crédits obtenus et des résultats scolaires.

Le candidat devra démontrer la pertinence et le caractère significatif de son expérience dans une lettre d'au moins 300 mots, et il devra se soumettre à une entrevue. Il pourra se voir imposer des cours d'appoint ou une propédeutique.

Nonobstant ce qui précède, un dossier dont la qualité est jugée exceptionnelle pourra être considéré pour l'admission.

PLAN DE FORMATION :

12 crédits optionnels

Cours optionnels

Choisir au moins 9 crédits (3 cours) dans les deux créneaux suivants, dont au moins 3 crédits (1 cours) dans chacun des créneaux:

Créneau télécommunication:

INF6263	Ingénierie des protocoles de communication
INF6223	Systèmes de communications multimédias

Créneau sécurité:

INF6103	Analyse et conception des protocoles de sécurité
INF6153	Systèmes de contrôle d'accès aux données
INF6163	Introduction à la cryptographie
INF6233	Sécurité informatique et méthodes formelles
INF6293	Éléments avancés en cryptographie

L'étudiant peut choisir un maximum de 3 crédits (1 cours) parmi la liste suivante:

INF6083	Sujets spéciaux
INF6273	Technologie avancée en télécommunication
INF6002	Systèmes à objets répartis
INF6003	Développement des applications client-serveur
INF6043	Algorithmique répartie
INF6123	Structures de données avancées
INF7093	Éléments avancés d'analyse d'images
INF6143	Bases de données avancées
INF6173	Conception de syst. temps-réel répartis embarqués
INF6323	Programmation infonuagique avancée
INF6243	Techniques d'apprentissage
INF6253	Web sémantique
INF6333	Éléments d'intelligence artificielle appliquée
INF6343	Intelligence artificielle distribuée

INF6002

Systèmes à objets répartis

Objectifs : Permettre à l'étudiant de maîtriser les connaissances nécessaires pour concevoir une infrastructure de systèmes répartis en considérant les nouvelles technologies et les normes associées, dont celles spécifiques à l'interopérationalité.

Contenu : Étude des architectures distribuées et essentiellement celles basées sur le modèle client/serveur et l'approche orientée objet. Développement de composants logiciels réutilisables, distribuables et interopérationnels indépendamment de la plate-forme matérielle et du langage de programmation respectifs du client et du serveur. Étude du standard CORBA (Common Object Request Broker Architecture) de l'OMG : bus, services, langage de définition d'interface (IDL), outils communs.

INF6003

Développement des applications client-serveur

Objectifs : Permettre à l'étudiant de maîtriser l'approche client-serveur et le familiariser avec la programmation des réseaux.

Contenu : Rappel sur les protocoles de transport pour la programmation: TCP/IP, UDP. Modèle Client-Serveur. Programmation des soquets. Appels de procédures à distance: modèle RPC. Présentation de données. Interfaces applicatives. Client-Serveur dans les bases de données SQL. Le transactionnel: protocoles 2PL, transactions réparties, standards de traitements de transactions. Interopérationalité. Autres types de serveur : serveurs de noms, serveurs d'informations (NIS).

INF6043

Algorithmique répartie

Objectifs : Permettre à l'étudiant d'analyser les différents algorithmes spécifiques au traitement réparti. Lui permettre d'évaluer leur efficience et leur complexité. Lui permettre d'acquérir une compréhension des méthodes générales qui sous-tendent l'algorithmique répartie.

Contenu : Concept d'algorithmes répartis. Mesures de complexité. Analyse de performance. Méthodes de validation. Algorithmes : de routage, d'élection, de synchronisation, de consensus (communication défaillante, processus défaillant, stabilisation), pour l'exclusion mutuelle, pour l'allocation des ressources, spécifiques aux réseaux asynchrones, pour snapshots. Applications aux réseaux de communication, bases de données réparties, etc.

INF6083

Sujets spéciaux

Objectifs : Permettre à l'étudiant d'acquérir des connaissances sur un (ou des) sujet(s) spécifique(s) pertinent(s) à son programme.

Contenu : Présentation d'une activité portant sur un (ou des) sujet(s) non couvert(s) dans les autres cours du programme. Activité offerte par un professeur ou une équipe de professeurs. Cette activité traite d'un ou de sujets d'intérêt et apporte une contribution particulière à la formation de l'étudiant. Le contenu de ce cours doit faire l'objet d'une approbation préalable par le Comité de programme.

INF6103

Analyse et conception des protocoles de sécurité

Objectifs : Permettre à l'étudiant d'avoir une bonne maîtrise des concepts, des langages, des méthodes modernes et des outils utilisés dans l'analyse et la spécification des protocoles de sécurité.

Contenu : Cryptographie. Protocoles de sécurité. Rôle des protocoles de sécurité dans les systèmes de communication et les systèmes distribués. Présentation de quelques protocoles existants. Propriétés de sécurité : confidentialité, authentification, anonymat, atomicité, non-répudiation, etc. Taxonomie des failles de sécurité. Langages formels pour la spécification des protocoles de sécurité CCS/CSP, SPI, BAN, SPC, etc. Techniques formelles de vérification et preuves de correction des protocoles de sécurité.

INF6123

Structures de données avancées

Objectifs : Permettre à l'étudiant de se familiariser avec les structures de données avancées et leur application pour la construction d'algorithmes efficaces. Approfondir ses connaissances en algorithmique à travers des problèmes à solutions complexes.

Contenu : Éléments de la théorie des graphes. Graphes planaires, leurs propriétés et applications. Approfondissement des dictionnaires et arborescences. Types des tas. Files de priorité. Médians. Approfondissement de la technique de programmation dynamique. Congruences et algorithmes de la théorie des nombres. Algorithmes de filtrage. Algorithmes avancés sur les graphes. Algorithmes géométriques.

INF6143

Bases de données avancées

Objectifs : Permettre aux étudiants de maîtriser les connaissances sur les fondements, concepts et problèmes reliés aux bases de données allant des bases de données conventionnelles (incluant les bases de données réparties) aux bases de données plus avancées comme les entrepôts de données et les bases multimédia (incluant les systèmes d'information géographique et les bases documentaires).

Contenu : Rappels sur les bases de données (BD). Contrôle et optimisation des performances dans un environnement centralisé. Bases de données réparties : principes, stratégies de conception, traitement des requêtes réparties, et gestion des transactions réparties. Veille économique (business intelligence) : fouille et entreposage de données. BD multimédia (particularités et exigences, stockage et exploitation, systèmes d'information géographique. BD documentaires). BD et Web (connexion à une BD via le Web, langage XML).

INF6153

Systèmes de contrôle d'accès aux données

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. Analyse de cohérence et complétude 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.

INF6163

Introduction à la cryptographie

Objectifs : Permettre aux étudiants de maîtriser les concepts de la cryptographie et de son application dans le domaine de la sécurité des données. Lui permettre d'analyser les différents algorithmes spécifiques à la cryptographie. Lui permettre d'évaluer leur efficacité et leur complexité, ainsi que d'acquérir une compréhension des méthodes générales de la cryptanalyse.

Contenu : Introduction à la cryptographie: terminologie, fonctions cryptographiques ; exemples historiques de protocoles de cryptographie : la cryptographie classique, le chiffrement de Vigenère, le chiffrement de Hill; la cryptanalyse des crypto-systèmes classiques. La cryptographie moderne, protocoles de confidentialité : protocoles à clé secrète et à clé publique. Introduction aux fonctions booléennes; opérateurs logiques et polynômes. Cryptographie à clé secrète; diagrammes de Feistel ; D.E.S., la version simplifiée S-DES ; I.D.E.A.; S-IDEA. Le protocole A.E.S., S-AES: modes d'opération des chiffrements par blocs. Cryptanalyse des protocoles à clé secrète : confusion et diffusion ; cryptanalyse linéaire. Introduction à la théorie des nombres; les nombres premiers appliqués aux crypto-systèmes asymétriques. Concept de cryptographie à clé publique; algorithme RSA, gestion des clés, algorithme Diffie-Hellman; fonctions de hachage, algorithmes SHA-1et MD5; authentification des messages. Signatures numériques, standard DSS, authentification des protocoles.

INF6173

Conception de syst. temps-réel répartis embarqués

Objectifs : Permettre aux étudiants de maîtriser les particularités des phases de développement des systèmes en temps réel répartis et particulièrement des systèmes embarqués. Lui permettre de tester ces systèmes et évaluer leur performance. Lui permettre également d'approfondir les connaissances relatives aux techniques d'ordonnancement et aux comportements des systèmes réactifs et leurs applications

Contenu : Rappel sur les concepts des systèmes temps réel. Introduction des systèmes temps réel distribués embarqués (STRDE). Analyse et conception des systèmes temps réel répartis, concept de Co-Design. Processeurs embarqués. Optimisation de la conception et du développement de systèmes temps réel répartis. Apport de l'approche orientée objet à la conception des systèmes temps réel répartis. Performance statique et dynamique. Multitraitement temps réel distribué, techniques d'ordonnancement, puissance dans les systèmes embarqués, accélérateurs de matériel, systèmes d'exploitation (QNX, ITRON, etc.). Langages de spécification, outils de simulation pour réseaux de capteurs (TOSSIM, etc.). Applications (routage, transport des données, etc.).

INF6223

Systèmes de communications multimédias

Objectifs : Permettre aux étudiants de maîtriser les systèmes de communications multimédias et les traitements associés. Lui permettre d'acquérir les connaissances de base pour le développement d'applications multimédias

Contenu : Introduction au multimédia, outils et interfaces. Représentation des données multimédias, audio, image et vidéo. Compression des données multimédias, algorithmes de base. Normes de codage JPEG et MPEG. Sécurité multimédia, watermarking, gestion numérique des droits (DRM), authentification, vidéosurveillance. Bases de données multimédias, recherche par le contenu. Applications : Multimédia et réseaux, protocoles de transfert, internet, réseaux sans-fil, transport en temps réel, synchronisation, qualité de service.

INF6233

Sécurité informatique et méthodes formelles

Objectifs : Permettre aux étudiants de maîtriser les techniques formelles utilisées pour la sécurisation des systèmes et réseaux informatiques

Contenu : Problèmes de la sécurité dans les logiciels et intergiciel. Formalismes algébriques et logiques pour la description des systèmes et des politiques de sécurité. Automates d'édition. Techniques formelles de renforcement de politiques de sécurité dans les systèmes. Renforcement par Monitorage. Renforcement par réécriture de programmes. Classes de propriétés de sécurités : sûreté, vivacité, « renewal », etc.

INF6243

Techniques d'apprentissage

Objectifs : Permettre aux étudiants de maîtriser les concepts fondamentaux de l'apprentissage automatique et d'appliquer ces notions à des problèmes concrets. Leur faire acquérir des connaissances sur les techniques d'apprentissage supervisé et non supervisé, les techniques d'apprentissage pour les données textuelles, les algorithmes de classement des pages Web.

Contenu : Concepts d'apprentissage supervisé : classification et régression, frontière de décision et fonctions discriminantes; Arbres de décision et techniques de traitement du sur-apprentissage (overfitting); Apprentissage par ensemble : (bagging), (boosting) et forêt d'arbres; Machine à noyaux : dimension VC et machines à supports vectorielles; Apprentissage non supervisé : (clustering), les mélanges de loi de distribution statistique, carte de Kohonen et algorithme SOFM; Apprentissage de données multidimensionnelles : techniques de réduction de la dimension, classification non supervisée dans les sous-espaces de dimension (subspace clustering); Fouille de données textuelles : modèle TF-IDF et analyse sémantique latente; Prospection du Web : algorithmes HITS et PageRank.

INF6253

Web sémantique

Objectifs : Permettre aux étudiants de maîtriser les principes qui sont à la base du Web sémantique. Lui fournir les connaissances nécessaires à la compréhension des technologies utilisées pour la réalisation du Web sémantique. Présenter l'état actuel du développement du Web sémantique et les perspectives de recherche dans ce domaine.

Contenu : Introduction au Web sémantique et son contenu. Techniques de représentation de connaissances mises en œuvre dans le cadre du Web sémantique. Frameworks de métadonnées. Ontologies et schéma. RDF. Logiques de description et OWL. Alignements et gestion des ontologies. Aspects computationnels du Web sémantique et introduction aux services Web. Sélection, composition et médiation des services sémantiques. Exemples pratiques. Au terme de ce cours, l'étudiant sera en mesure de : comprendre les enjeux liés à la réalisation du Web sémantique; construire une ontologie dans le but d'une intégration au Web sémantique; construire une application simple pour le Web sémantique; comprendre les défis techniques liés à la réalisation du Web sémantique; comprendre aisément les travaux de recherche et développement qui portent sur le Web sémantique.

INF6263

Ingénierie des protocoles de communication

Objectifs : Permettre aux étudiants de maîtriser le processus d'ingénierie, de conception formelle, de validation et test des protocoles de communication.

Contenu : Fonctions des protocoles de communication. Modèles à couches : protocoles et services. Contrôle d'erreur. Contrôle de flux. Gestion des connexions. Spécification formelle des protocoles de communication. Validation des protocoles de communication. Techniques à états finis et algébriques : analyse d'accessibilité, équivalence par test, équivalence observationnelle, etc. Évaluation de modèles. Méthodes de test. Étude de quelques langages formels ou semi-formels tel que : CCS. Pi-Calculus, LOTOS, PROMELA, SDL, UML. Application avec outils, comme SPIN, CADP, ALLOY, etc.

INF6273

Technologie avancée en télécommunication

Objectifs : Permettre aux étudiants de comprendre le fonctionnement et les protocoles récents des systèmes modernes de télécommunication, particulièrement des réseaux à très haut débit et les familiariser avec les récents développements et applications dans ce domaine.

Contenu : Revue des architectures des réseaux de télécommunication. Réseaux locaux (LAN), métropolitains (MAN), étendus (WAN). Technologie Mode de transfert asynchrone (ATM). Communication par fibres optiques et standard SONET (Synchronous Optical Network). Réseaux tout optiques. Communications et réseaux sans fil. Réseaux ad-hoc. Méthodes de contrôle d'accès multiples. Gestion de la performance des réseaux modernes. Contrôle de congestion dans les réseaux à très haut débit. Réseaux cognitifs. Applications.

INF6293

Éléments avancés en cryptographie

Objectifs : Maîtriser les techniques avancées de cryptologie répondant à des critères spécifiques de sécurité et de performance. Apprendre et maîtriser les fondements mathématiques et l'analyse de ces techniques et leurs implications sur la sécurité.

Contenu : Rappel sur les systèmes de chiffrement symétriques et asymétriques. Rappel des notions d'algèbre et de théorie des nombres. Cryptographie basée sur les logarithmes discrets (cryptographie à courbes elliptiques, ElGamal, DSA, échange de clés Diffie-Hellman, etc.). Fonctions de hachage (MD5, SHA-1, etc.). Cryptographie à seuil. Cryptographie basée sur l'identité. Cryptanalyse. Partage de secrets. Éléments de cryptographie quantique.

INF6323

Programmation infonuagique avancée

Objectifs : Apprendre et maîtriser les concepts et les techniques de l'infonuagique et des mégadonnées. Concevoir et implémenter des applications pratiques de science des données sur des plateformes infonuagiques.

Contenu : Modélisation des données avec XML et JSON. Services Web de type SOAP. Services Web de type REST. Introduction à l'infonuagique. Modèles de services en infonuagique (logiciel-service, plateforme-service, infrastructure-service, fonction-service, etc.). Modèles de déploiement de l'infonuagique (privé interne, privé externe, public, communautaire, multi-cloud et hybride). Techniques de virtualisation en infonuagique (virtualisation par machines virtuelles et virtualisation par conteneurs). Programmation infonuagique (Amazon Web Services et Google Cloud Platform). L'écosystème Hadoop : le système de fichiers distribué HDFS, le gestionnaire de ressources YARN, le modèle de programmation MapReduce. L'écosystème Apache Spark pour l'analyse des données en temps réel. Bases de données non relationnelles NoSQL. Le système MongoDB de gestion de bases de données orientées documents.

INF6333

Éléments d'intelligence artificielle appliquée

Objectifs : Permettre aux étudiants d'approfondir les techniques de base de l'apprentissage machine et les aspects pratiques de l'intelligence artificielle (IA). Comprendre les enjeux spécifiques liés aux données et à l'évaluation de performance dans la conception et le développement d'applications basées sur l'IA.

Contenu : Acquisition, extraction, visualisation et préparation des données. Extraction de caractéristiques, réduction de la dimensionnalité, et représentation des connaissances. Problèmes de déséquilibre de données. Apprentissage supervisé, non-supervisé et par renforcement. Réseaux de neurones et apprentissage profond. Apprentissage d'ensemble et prise de décision. Déploiement de solutions basées sur l'intelligence artificielle. Enjeux dans la conception et le développement des systèmes intelligents embarqués et des systèmes intelligents en temps réel. Critères de performances et évaluation d'applications basées sur l'intelligence artificielle. Études d'applications dans les domaines de la vision artificielle, de la robotique, du génie, des soins de santé et du forage de données.

INF6343

Intelligence artificielle distribuée

Objectifs : Dans le contexte de l'intelligence artificielle, permettre aux étudiant(e)s de maîtriser les principaux défis liés à l'interaction d'agents autonomes. Présenter aux étudiant(e)s les principales théories et outils pour opérationnaliser ces interactions, notamment les protocoles formels, la théorie des jeux, et l'apprentissage multi-agent.

Contenu : La notion d'agent et d'architecture multi-agents dans le contexte de l'intelligence artificielle distribuée. Les principaux défis des interactions entre agents : coordination, communication, apprentissage. Modèles d'organisations multi-agents : institutions électroniques, protocoles formels. La notion de machine sociale. Modélisation des interactions entre agents : théorie des jeux coopératifs et non coopératifs. Mécanismes de coordination : choix collectif, mécanismes d'incitation, systèmes de réputation. Aspects algorithmiques des décisions collectives, concepts d'équité. Apprentissage par renforcement, apprentissage multi-agent. Applications dans différents domaines, dont la cyber sécurité, les réseaux et la robotique.

INF7093

Éléments avancés d'analyse d'images

Objectifs : Permettre à l'étudiant de : Connaître le processus de formation d'images. Maîtriser les outils fondamentaux d'analyses et de traitement des images. Maîtriser différents algorithmes pour l'extraction de caractéristiques et la représentation des images. Réaliser des projets basés sur le traitement d'images, tels que la reconnaissance d'objets, la segmentation, la classification d'images, le codage et la compression.

Contenu : Aspects avancés des systèmes d'acquisition, du processus d'échantillonnage, de quantification et de filtrage des images. Techniques d'extraction de différentes caractéristiques (ex. les contours, les régions et les formes). Opérations de base pour l'amélioration de la qualité des images (la restauration et le rehaussement). Algorithmes de recalage et d'estimation du mouvement dans les séquences d'images. Aspects de haut niveau, tels que la représentation et la classification d'images.