
INF8750

Sécurité des systèmes informatiques

Plan de cours

Responsable(s) du cours

GAMBS, Sébastien
PK-4925
gambs.sebastien@uqam.ca
<https://sebastiengambs.openum.ca>
Groupes : 050

Méthodes de communication

Moodle servira à centraliser les informations liées au cours et les cours synchrones se feront en mode comodal (en présentiel et sur Zoom), j'utiliserais aussi le courriel du groupe cours pour des informations générales.

Si vous assistez à distance, si possible (par exemple si votre connexion vous le permet) et si vous êtes confortable avec cela (par exemple si vous êtes dans un environnement calme), je vous encourage à ouvrir votre caméra vidéo pour faciliter les interactions. Vous pouvez aussi utiliser un arrière-fond virtuel pour remplacer l'image en arrière-plan de votre domicile.

Si une question concernant un aspect du cours pourrait intéresser tout le monde de manière globale, n'hésitez pas à la poser durant le cours ou sur le forum du cours sur Moodle.

Vous pouvez aussi utiliser le courriel (réponse en 24h à 48h heures ouvrables) ou encore prendre rendez-vous avec moi pour une rencontre virtuelle.

Auxiliaires d'enseignement (en charge des laboratoires) : Guillaume Gagnon (gagnon.guillaume.5@courrier.uqam.ca), Sofiane Azogagh (azogagh.sofiane@courrier.uqam.ca).

Modalités d'enseignement

Pour cette session, l'enseignement se fera en distanciel pendant les premières semaines puis en comodal par la suite (cela dépendra évidemment de l'évolution de la situation Covid). Il y aura aussi chaque semaine une capsule de 30 minutes à regarder de manière asynchrone avant le cours du vendredi.

- Capsules (asynchrone) : chaque semaine le mardi matin au plus tard une capsule vidéo d'une durée totale de 30 minutes sera rendue disponible. Cette capsule concernent des préliminaires pour le cours de vendredi et doivent être consultées en avance.
- Cours magistraux (synchrone) : vendredi de 9h30 à 12h30. Le cours magistral complètera et approfondira le matériel vu dans les capsules.
- Laboratoires (synchrone) : vendredi de 13h30 à 15h30. Typiquement une mise en pratique et validation expérimentale de sujets vus en cours mais parfois aussi une approfondissement théorique.

Local du cours

- PK-R220 / Zoom le vendredi de 9h30-12h30 pour le cours magistral (voir le lien Zoom sur le Moodle du cours).
- PK-S1560 / Zoom le vendredi de 13h30-15h30 pour le laboratoire (voir le lien Zoom sur le Moodle du cours).

Responsabilité des étudiants

Il est attendu des étudiants qu'ils visionnent les capsules et assistent à chaque cours magistral et laboratoire. Il est aussi attendu des étudiants qu'ils lisent le matériel de cours (incluant les lectures supplémentaires) et qu'ils participent activement dans les discussions de classe.

Dates importantes

- 24 janvier 2022 : date limite pour annulation sans facturation.
- 14 mars 2022 : date limite pour abandon sans mention d'échec, avec facturation.

Description du cours

Principes et concepts fondamentaux de la sécurité des systèmes informatiques. Principaux services : confidentialité, intégrité, disponibilité, authentification, non répudiation, contrôle d'accès. Typologie des attaques : fuites, modifications d'information, privations de service. Mécanismes sécuritaires modernes : systèmes de chiffage symétriques et asymétriques ; fonctions de hachage ; génération pseudo-aléatoire. Protocoles sécuritaires : authentification, signature, échange et gestion de clés. Sécurité des systèmes centralisés et des systèmes répartis : politiques et modèles de sécurité ; contrôle d'accès ; rôles et privilèges. Sécurité des programmes : virus, chevaux de Troie. Contre-mesures : journalisation, audits ; détection d'intrusion ; filtrage ; mécanismes de recouvrement. Analyse de risque. Éducation des usagers. Considérations légales, politiques et éthiques.

Objectif du cours

Avec la croissance fulgurante que connaît le monde des télécommunications, entraînée par la locomotive Internet et stimulée par la pénétration des technologies de transmission sans fil, la problématique de la sécurité des données et des processus prend de nos jours une importance cruciale. On abordera dans ce cours le très vaste sujet de la sécurité informatique, en s'intéressant aux principes fondamentaux, aux mécanismes permettant d'assurer des services de sécurité, de même qu'aux applications concrètes rencontrées dans les derniers déploiements technologiques.

Le but premier du cours est de sensibiliser l'étudiant à la problématique de la sécurité dans un système informatique. Par la suite, par l'étude des principaux problèmes de sécurité et de leurs solutions possibles, on sera à même d'apprécier la complexité inhérente qui sous-tend la guerre perpétuelle que se livrent les attaquants et les défenseurs dans le monde de l'information électronique.

Les compétences développées dans le cadre de ce cours rendront l'étudiant capable de :

- Définir les propriétés fondamentales de la sécurité informatique tels que *confidentialité, authentification, intégrité, non-répudiation, disponibilité et respect de la vie privée*.
- Énoncer les principes fondamentaux qui gouvernent l'établissement de services sécuritaires.
- Décrire, expliquer le fonctionnement et mettre en oeuvre les principaux algorithmes cryptographiques pour le chiffrement, le hachage, l'authentification de messages et la signature électronique.
- Décrire les caractéristiques des systèmes de chiffrement à clé secrète et à clé publique.
- Décrire et comprendre des protocoles cryptographiques courants utilisés pour la sécurité informatique.
- Effectuer une analyse de risque, en fonction d'un contexte de fonctionnement spécifique et d'hypothèses sur les capacités de l'attaquant et les menaces possibles.
- Identifier les particularités des menaces contre la sécurité d'un système selon le contexte centralisé ou distribué de ce système.
- Proposer des contre-mesures selon les menaces envisagées.

Contenu du cours

- Introduction : Problématique de la sécurité : confidentialité, authentification, intégrité, disponibilité, non-répudiation, respect de la vie privée, contrôle d'accès. Vulnérabilités, menaces à la sécurité et attaques. Attaques conduisant à des fuites d'information (divulgaration de contenu, analyse de trafic), à des modification d'information (modifications de contenu ou d'ordre des messages, reprises de messages), à des privations de service (retard de messages, destruction).
- Techniques de base en sécurité : Terminologie. Notion de confiance. Analyse de risque. Principes et politiques de sécurité. Éducation des usagers. Contre-mesures : Journaux de bord (logs) et audits. Détection d'intrusion. Filtrage. Mécanismes de recouvrement. Analyse de risque. Principes et politiques de sécurité. Éducation des usagers.
- Authentification par mot de passe. Fonctions de hachage (MD5, SHA-1, SHA-3). Stockage sécurisé de mots de passe. Politique de composition de mots de passe. Quantification de la sécurité des mots de passe. Craquage de mots de passe. Authentification par biométrie.

- Chiffrement symétrique. Principes de Kerckhoffs. Exemples de chiffrements historiques et de mécanismes de base : transposition, permutation. Caractérisation des systèmes de chiffrement. Cryptanalyse et attaques. Notions de base fondamentales : entropie, redondance. Chiffrement à sécurité inconditionnelle : masque jetable. Systèmes de chiffrement symétriques modernes (DES, AES). Modes de fonctionnement : ECB, CBC, CTR. Chiffrement par flux (RC4).
- Authentification de messages. Codes d'authentification de message (HMAC, CBC-MAC). Introduction aux protocoles d'authentification. Protocole : authentification mutuelle directe, authentification par serveur de confiance.
- Chiffrement asymétrique (clé publique : RSA, Diffie-Hellman, DSA). Fonctions à sens unique. Intégrité des données et authentification de messages. Génération pseudo-aléatoire. Signature numérique.
- Échange et gestion de clés. Tiers de confiance. Authentification par défi et réponse. Protocoles à divulgation nulle de connaissances. Infrastructures de distribution et de gestion de clés. Certificats : X.509.
- Étude détaillée de protocoles de sécurité : TLS, PGP.
- Sécurité des systèmes répartis et de réseaux : Menaces spécifiques : écoute illicite, imposture, déni de service, brouillage. Caractéristiques des médiums de transmission. Gestion de la confiance. Autorisation décentralisée. Pare-feu. Réseaux privés virtuels. Authentification dans les réseaux Wi-Fi (WEP, WPA et WPA2).
- Respect de la vie privée. Lien avec la sécurité informatique. Outil de traçage, traces numériques. Attaques par inférence et méthodes d'assainissement. Technologies de protection de la vie privée (réseaux de communication anonyme, accréditations anonymes, retrait privé d'information).

Modalités d'évaluation

Description sommaire	Date	Pondération
Participation en classe		5 %
Actualité de sécurité	Une fois	5 %
Devoirs et travaux pratiques	Périodique	30 %
Présentation article	Une fois	20 %
Travail de session	Voir calendrier ci-bas	40 %

La note global de passage pour le cours est de 60 %.

Présentation d'une actualité de sécurité (5%)

Chaque semaine en début du cours (à partir du cours 4), deux étudiants présenteront une actualité liée à la sécurité en 5 minutes chacun. L'objectif principal de ce travail est de présenter un problème actuel de sécurité de manière concise mais tout en allant plus loin que simplement un article de vulgarisation.

Devoirs notés et travaux pratiques (30 %, 10% par devoir)

Au cours de la session, trois devoirs écrits notés permettront aux étudiants d'approfondir les sujets vus en cours ou encore de mettre en pratique et de vérifier expérimentalement certains des concepts présentés en classe. Les devoirs et travaux, qui pourront être réalisés en *équipes de deux*, toucheront à différents sujets de la sécurité informatique. Il pourra y avoir de la programmation à effectuer, mais pas de développements majeurs. L'objectif principal des devoirs est de permettre de consolider les notions apprises pendant le cours.

Présentation d'un article scientifique (20 %)

Chaque semaine à partir du cours 5, deux ou trois étudiants vont présenter chacun un article de recherche sous la formule d'une capsule pré-enregistrée (20 minutes de présentation). L'objectif de ce travail est de se familiariser avec la recherche académique sur le sujet et de pouvoir le restituer de manière pédagogique.

Travail de session (projet) (40 %)

Comme nous aborderons un domaine beaucoup plus vaste que ce qu'il est possible de couvrir durant le temps limité qui est alloué au cours, un travail de longue haleine, réalisé dans le cadre du cours, vous permettra d'en approfondir un aspect particulier à votre choix. Ce travail peut prendre diverses formes : compte-rendu de lectures, application pratique de notions vues en classe, réalisation de logiciel ou de matériel, etc. Le produit fini devra de toute façon comporter un rapport, qui rendra compte de votre travail et permettra de démontrer ce que vous avez pu apprendre au-delà de ce qui est couvert en classe.

Vous devrez d'abord sélectionner un sujet, qui sera ensuite approuvé par le professeur.

Pour faire ce choix, on peut :

- penser à un aspect de l'informatique ou des télécommunications et de le relier au concept de sécurité
- discuter avec des collègues étudiants ou de travail pour des suggestions
- songer à l'amélioration de la sécurité d'un système sur lequel vous travaillez
- consulter un (des) articles intéressants sur la sécurité

Les principales revues traitant de sécurité informatique sont : Computers & Security, Journal of Computer Security, mais on trouve des articles sur le sujet dans plusieurs autres revues. Les principales conférences sont Crypto et Eurocrypt (pour la cryptographie), Symposium on Research in Security and Privacy, National Computer Security Conference, Annual Computer Security Applications Conference ainsi que European Symposium on Research in Computer Security.

Quelques suggestions de sujets (liste non-exhaustive) :

- Anonymat, vie privée et confidentialité
- Aspects sécuritaires de systèmes d'exploitation connus
- Authentification dans un environnement distribué
- Cartes à puce pour la sécurité
- Éthique informatique
- Gestionnaires de licences pour logiciels
- Pares-feu, contrôle d'accès par listes
- Prévention et détection d'intrusion avancée
- Sécurité et bases de données
- Sécurité et commerce électronique
- Sécurité et réseaux sans fil/ad hoc
- Stéganographie, copyright et protection contre la copie
- Virus
- Nuisances (pourriels, adware, etc.)
- Systèmes leurres (honey-pots)
- Réseaux de zombies (botnets)
- Virtualisation et techniques de méta-surveillance
- Tests de Turing inversés (CAPTCHA)

Principaux jalons et éléments à remettre :

- Semaine 5 : Vous devez avoir fait le choix définitif du sujet. Vous devez remettre un document de 1 page expliquant ce que vous voulez faire et pourquoi. Vous devez fournir plusieurs sources bibliographiques et décrire comment vous comptez vous y prendre pour compléter le projet. *(4 % de la note du projet)*
- Semaine 8 : Votre projet doit être relativement bien avancé. Vous devez remettre un plan détaillé précisant ce que vous faites, comment et quels sont les résultats spécifiques que vous attendez. De plus, vous devez justifier la pertinence de votre travail et indiquer comment votre travail peut être d'intérêt général. *(16 % de la note du projet)*
- Semaines 13, 14 et 15 : Séance de présentations. Chaque étudiant prépare une présentation décrivant de manière synthétique son travail. Chaque étudiant prépare une présentation décrivant de manière synthétique son travail qui se fera en direct (20 minutes de présentation + 10 minutes de questions). *(40% de la note du projet)*
- Semaine 15 : Remise du rapport final. Le produit fini doit être d'assez bonne qualité pour être soumis à un magazine ou à votre supérieur au travail. *(40 % de la note du projet)*

Prenez note que la correction des devoirs tient abondamment compte des développements. Il est donc avantageux d'exposer votre démarche de travail. Une réponse correcte obtenue au terme d'un raisonnement invalide ne vaut pas grand chose. Par contre, un raisonnement valide, conduisant à une réponse erronée à cause d'erreurs mineures vaut beaucoup plus. Dans le doute, il vaut mieux être explicite que succinct.

Les règlements de l'UQAM concernant le plagiat seront strictement appliqués. Pour plus de renseignements, consultez le site suivant : <http://www.sciences.uqam.ca/etudiants/integrite-academique.html>

Tout travail que vous soumettez doit être le fait de votre propre travail. Vous pouvez échanger avec vos collègues sur les travaux, les approches de solutions, mais les idées et solutions que vous soumettez doivent émaner de votre propre réflexion. Dans le cas de programmes, vous devez créer et coder votre propre code source, et le documenter vous même. Une fois le programme écrit, il est possible de se faire aider pour le débogage.

En cas de doute sur l'originalité des travaux, un test oral pourra être exigé.

Une pénalité de retard de 10% par jour ouvrable sera appliquée sur les travaux remis après les dates prévues. Il est de la responsabilité de l'étudiant de se faire des copies de ses travaux.

Médiagraphie

Sera complété au fur et à mesure des lectures.

Politique d'absence aux examens

Reprise d'examen. L'autorisation de reprendre un examen en cas d'absence est de **caractère exceptionnel**. Pour obtenir un tel privilège, l'étudiant.e doit avoir des motifs sérieux et bien justifiés.

Conflits d'horaire. Il est de la responsabilité de l'étudiant.e de ne pas s'inscrire à des cours qui sont en conflit d'horaire, tant en ce qui concerne les séances de cours ou d'exercices que les examens. **De tels conflits d'horaire ne constituent pas un motif justifiant une demande d'examen de reprise.**

Procédure. L'étudiant.e absent.e lors d'un examen doit, dans les cinq (5) jours ouvrables suivant la date de l'examen, présenter une demande de reprise en utilisant le formulaire prévu, disponible sur <http://info.uqam.ca/repriseexamen/>.

Pièces justificatives. Dans le cas d'une absence pour raison médicale, l'étudiant.e doit joindre un certificat médical original et signé par le médecin décrivant la raison de l'absence à l'examen. Les dates d'invalidité doivent être clairement indiquées sur le certificat. Une vérification de la validité du certificat pourrait être faite. Dans le cas d'une absence pour une raison non médicale, l'étudiant.e doit fournir les documents originaux expliquant et justifiant l'absence à l'examen ; par exemple, lettre de la Cour en cas de participation à un jury, copie du certificat de décès en cas de décès d'un proche, etc. Toute demande incomplète sera refusée. Si la direction du programme d'études de l'étudiant.e constate qu'un.e étudiant.e a un comportement récurrent d'absence aux examens, l'étudiant.e peut se voir refuser une reprise d'examen.

Pour plus d'informations. Consulter la page <http://info.uqam.ca/politiques>.

Règlement numéro 18 sur les infractions de nature académique (extraits)

Tout acte de plagiat, fraude, copiage, tricherie ou falsification de document commis par une étudiante, un étudiant, de même que toute participation à ces actes ou tentative de les commettre, à l'occasion d'un examen ou d'un travail faisant l'objet d'une évaluation ou dans toute autre circonstance, constituent une infraction au sens de ce règlement.

La liste non limitative des infractions est définie comme suit :

- la substitution de personnes ;
- l'utilisation totale ou partielle du texte d'autrui en la faisant passer pour sien ou sans indication de référence ;
- la transmission d'un travail pour fins d'évaluation alors qu'il constitue essentiellement un travail qui a déjà été transmis pour fins d'évaluation académique à l'Université ou dans une autre institution d'enseignement, sauf avec l'accord préalable de l'enseignante, l'enseignant ;
- l'obtention par vol, manoeuvre ou corruption de questions ou de réponses d'examen ou de tout autre document ou matériel non autorisés, ou encore d'une évaluation non méritée ;
- la possession ou l'utilisation, avant ou pendant un examen, de tout document non autorisé ;
- l'utilisation pendant un examen de la copie d'examen d'une autre personne ;
- l'obtention de toute aide non autorisée, qu'elle soit collective ou individuelle ;
- la falsification d'un document, notamment d'un document transmis par l'Université ou d'un document de l'Université transmis ou non à une tierce personne, quelles que soient les circonstances ;
- la falsification de données de recherche dans un travail, notamment une thèse, un mémoire, un mémoire-crédation, un rapport de stage ou un rapport de recherche ;
- Les sanctions reliées à ces infractions sont précisées à l'article 3 du Règlement no 18.

Les règlements concernant le plagiat seront strictement appliqués. Pour plus de renseignements :

- <http://www.infosphere.uqam.ca/rediger-un-travail/eviter-plagiat>
- <http://r18.uqam.ca/>

Politique no 16 visant à prévenir et combattre le sexisme et les violences à caractère sexuel

Les violences à caractère sexuel se définissent comme étant des comportements, propos et attitudes à caractère sexuel non consentis ou non désirés, avec ou sans contact physique, incluant ceux exercés ou exprimés par un moyen technologique, tels les médias sociaux ou autres médias numériques. Les violences à caractère sexuel peuvent se manifester par un geste unique ou s'inscrire dans un continuum de manifestations et peuvent comprendre la manipulation, l'intimidation, le chantage, la menace implicite ou explicite, la contrainte ou l'usage de force.

Les violences à caractère sexuel incluent, notamment :

- la production ou la diffusion d'images ou de vidéos sexuelles explicites et dégradantes, sans motif pédagogique, de recherche, de création ou d'autres fins publiques légitimes ;
- les avances verbales ou propositions insistantes à caractère sexuel non désirées ;
- la manifestation abusive et non désirée d'intérêt amoureux ou sexuel ;
- les commentaires, les allusions, les plaisanteries, les interpellations ou les insultes à caractère sexuel, devant ou en l'absence de la personne visée ;
- les actes de voyeurisme ou d'exhibitionnisme ;
- le (cyber) harcèlement sexuel ;
- la production, la possession ou la diffusion d'images ou de vidéos sexuelles d'une personne sans son consentement ;
- les avances non verbales, telles que les avances physiques, les attouchements, les frôlements, les pincements, les baisers non désirés ;
- l'agression sexuelle ou la menace d'agression sexuelle ;
- l'imposition d'une intimité sexuelle non voulue ;
- les promesses de récompense ou les menaces de représailles, implicites ou explicites, liées à la satisfaction ou à la non-satisfaction d'une demande à caractère sexuel.

Pour consulter la politique no 16

https://instances.uqam.ca/wp-content/uploads/sites/47/2018/05/Politique_no_16.pdf

Pour obtenir de l'aide, faire une divulgation ou une plainte

Bureau d'intervention et de prévention en matière de harcèlement
514-987-3000, poste 0886

Pour obtenir la liste des services offerts à l'UQAM et à l'extérieur de l'UQAM

<https://harcelement.uqam.ca>

Soutien psychologique (Services à la vie étudiante)

514-987-3185
Local DS-2110

CALACS Trêve pour Elles – point de services UQAM

514 987-0348
calacs@uqam.ca
<http://trevepourelles.org>

Service de la prévention et de la sécurité

514-987-3131

Politique no 44 d'accueil et de soutien des étudiant.e.s en situation de handicap

Politique. Par sa politique, l'Université reconnaît, en toute égalité des chances, sans discrimination ni privilège, aux étudiant.e.s en situation de handicap, le droit de bénéficier de l'ensemble des ressources du campus et de la communauté universitaire, afin d'assurer la réussite de leurs projets d'études, et ce, dans les meilleures conditions possibles. L'exercice de ce droit est, par ailleurs, tributaire du cadre réglementaire régissant l'ensemble des activités de l'Université.

Responsabilité de l'étudiant.e. Il incombe aux étudiant.e.s en situation de handicap de rencontrer les intervenant.e.s (conseiller.ère.s à l'accueil et à l'intégration du Service d'accueil et de soutien des étudiant.e.s en situation de handicap, professeur.e.s, chargé.e.s de cours, direction de programmes, associations étudiantes concernées, etc.) qui pourront faciliter leur intégration à la communauté universitaire ou les assister et les soutenir dans la résolution de problèmes particuliers en lien avec les limitations entraînées par leur déficience.

Service d'accueil et de soutien aux étudiant.e.s en situation de handicap. Le Service d'accueil et de soutien aux étudiant.e.s en situation de handicap (SASESH) offre des mesures d'aménagement dont peuvent bénéficier certains étudiant.e.s. Il est fortement recommandé aux de se prévaloir de ces services afin de réussir ses études, sans discrimination. Pour plus d'information, visiter le site de ce service : <https://vie-etudiante.uqam.ca/etudiant-situation-handicap/nouvelles-ressources.html> et celui de la politique institutionnelle d'accueil et de soutien aux étudiant.e.s en situation de handicap : https://instances.uqam.ca/wp-content/uploads/sites/47/2018/05/Politique_no_44.pdf

Il est important d'informer le SASESH de votre situation le plus tôt possible :

- En personne : 1290, rue Saint-Denis, Pavillon Saint-Denis, local AB-2300
- Par téléphone : 514 987-3148
- Par courriel : situation.handicap@uqam.ca
- En ligne : <https://vie-etudiante.uqam.ca/>