INF4471
Introduction à la sécurité informatique

Plan de cours

Responsable(s) du cours

Coordination : GAMBS, Sébastien
PK-4925
poste 0906
gambs.sebastien@uqam.ca
https://sebastiengambs.openum.ca

Description du cours

Principes et concepts fondamentaux de la sécurité des systèmes informatiques. Principaux objectifs de sécurité : confidentialité, intégrité, disponibilité, authentification, non-répudiation, contrôle d'accès. Typologie des attaques et menaces : fuites, modifications, dénis de service.

Introduction aux mécanismes de sécurité modernes : systèmes de chiffrage symétriques et asymétriques ; codes d'authentification de messages et signatures électroniques ; fonctions de hachage ; protocoles sécuritaires : authentification, contrôle d'accès.

Sécurité des réseaux : gestion et infrastructure de clés ; étude de la sécurité de protocoles existants (TLS, IPSec) ; protocoles d'authentification dans les réseaux sans fil (WEP, WPA et WPA2) ; surveillance et détection d'intrusion ; appareils mobiles.

Sujets avancés : introduction à la protection de la vie privée ; sécurité en infonuagique ; sécurité de l'internet des objets ; Bitcoin et blockchain.

Gestion des incidents de sécurité et améliorations des systèmes : mécanismes de recouvrement. Analyse de risque. Gestion des vulnérabilités techniques. Éducation des usagers. Considérations légales, politiques et éthiques. Politiques et modèles de sécurité.

Objectif du cours

Introduire les étudiants aux différents aspects de la sécurité des systèmes informatiques. Sensibiliser les étudiants aux risques et menaces. Présenter les techniques permettant d'assurer la sécurité des systèmes d'information. Décrire les méthodes de mitigation du risque.

À la fin de ce cours, l'étudiant devra être en mesure de :

- distinguer les principaux objectifs de sécurité ;
- expliquer le fonctionnement et justifier l'utilisation des principaux mécanismes de sécurité : chiffrement, signature, hachage, protocoles, etc. ;
- identifier les risques et les menaces auxquels fait face un système ;
- proposer des mesures de contrôle appropriées.

Contenu du cours

Introduction : Problématique de la sécurité : confidentialité, authentification, intégrité, disponibilité, non-répudiation, respect de la vie privé, contrôle d'accès. Vulnérabilités, menaces à la sécurité et attaques. Attaques conduisant à des fuites d'information (divulgation 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.

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

- Examen intra (22 octobre) : 30%
- Devoirs (étalés sur toute la session) : 40%
- Examen final (10 décembre) : 30%

Examen intra (30 %)

Examen à livre ouvert, portant sur la matière vue pendant la première moitié de la session.

Devoirs notés et travaux pratiques (40 %)

Occasionnellement au cours de la session, des devoirs écrits notés ou des travaux pratiques 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 en sécurité informatique. Il pourra y avoir de la programmation à effectuer, mais pas de développements majeurs.

Examen final (30 %)

Examen à livre ouvert, portant sur l'ensemble de cours.

Prenez note que la correction des exercices et examens tient abondamment compte des développements. Il est donc avantageux d'exposer votre 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.

Notes

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 déboguage.

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.

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.
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.**
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 étudiant a un comportement récurrent d'absence aux examens, l'étudiant-e peut se voir refuser une reprise d'examen.
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 le site Web du département à l'adresse suivante : info.uqam.ca/politiques/.
L'étudiant-e doit déposer le formulaire dûment complété au secrétariat de la direction de son programme d'études : PK-3150 pour les programmes de premier cycle, PK-4150 pour les programmes de cycles supérieurs. Pour plus de détails sur la politique d'absence aux examens du Département d'informatique, consultez le site web suivant : info.uqam.ca/politiques.

PLAGIAT Règlement no 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'évaluatiion 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 persone, quelles que aoient les circonstances ;**
- **la falsification de données de recherche dans un travail, notamment une thèse, un mémoire, un mémoire-création, un rapport de stage ou un rapport de recherche ;**
- **Les sanctions reliées à ces infrations sont précisées à l'article 3 du Règlement no 18.**

Les règlements concernant le plagiat seront strictement appliqués. Pour plus de renseignements, veuillez consulter les sites suivants : www.sciences.uqam.ca/etudiants/integrite-academique.html et www.bibliotheques.uqam.ca/plagiat/le-plagiat-liens-rapides.

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

Pour consulter la politique no 16 :

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

Services offerts :

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 la liste des services offerts en matière de violence sexuelle à l'UQAM et à l'extérieur de l'UQAM : harcelement.uqam.ca

CALACS Trêve pour Elles – point de services UQAM :
514 987-0348
calacs@uqam.ca
trevepourelles.org

Soutien psychologique (Services à la vie étudiante) :
514 987-3185
Local DS-2110

Service de la prévention et de la sécurité : 514 987-3131

Les étudiants qui ont une lettre signée de leur conseillère ou conseiller de l'Accueil et de soutien aux étudiants en situation de handicap (ASESH), dans laquelle il est fait état de leur inscription au ASESH à titre d'étudiant(e) en situation de handicap, sont invités à remettre ce document à leurs professeur(e)s et chargé(e)s de cours dès le début de la session afin que les aménagements dans le respect des exigences académiques soient déterminées de concert avec chacun des professeur(e)s et chargé(e)s de cours. Les étudiants qui ont une déficience et qui ne seraient pas inscrits au ASESH sont priés de se présenter au AB-2300.
Étudiants avant une déficience de type visuelle, auditive, motrice, trouble d'apprentissage, trouble envahissant du développement et trouble de santé mentale :
Les étudiant(e)s qui ont une lettre d'*Attestation des mesures d'aménagements académiques* obtenue auprès d'une conseillère, d'un conseiller de l'ACCUEIL ET SOUTIEN AUX ÉTUDIANTS EN SITUATION DE HANDICAP (ASESH) doivent rencontrer leurs enseignant(e)s au début de la session afin que des mesures d'aménagement en classe ou lors des évaluations puissent être mises en place. Ceux et celles qui ont une déficience ou une incapacité mais qui n'ont pas cette lettre doivent contacter l'ASESH au (514) 987-3148 ou se présenter au AB-2300 le plus tôt possible.