GROUPE 30 BÉGIN, Guy begin.guy@uqam.ca (514) 987-3000 4081 PK-4825

Mercredi, de 17h30 à 20h30 – Mercredi, 20h30 à 22h00 (ateliers) – Vendredi, 17h30 à 19h00 (ateliers)

DESCRIPTION

Ce cours vise à sensibiliser les étudiants aux différents aspects de la sûreté de fonctionnement et de la sécurité des systèmes, et à développer chez eux les compétences nécessaires à la prise en charge de ces objectifs essentiels dans le contexte des systèmes embarqués. Problématique d'ensemble de la sécurité et de la sûreté de fonctionnement d'un système embarqué. Causes : fautes, défaillances, erreurs, attaques, ergonomie. Fiabilité de système, de matériel, de logiciel : MTTF, MTTR, MTBF. Critères de sûreté de fonctionnement : fiabilité, disponibilité, innocuité, maintenabilité, testabilité. Mécanismes de contrôle : tolérance aux fautes, suppression des fautes, conception pour la sûreté. Menaces, vulnérabilités, attaques, préjudice, contrôles. Objectifs de sécurité : confidentialité, authenticité, intégrité, disponibilité. Mécanismes sécuritaires : chiffrage symétrique et asymétrique, hachage, fonctions à sens unique. Protocoles sécuritaires : authentification, échange de clés, signature. Notion de confiance. Contrôle d'accès, inviolabilité. Matériel spécialisé : cartes à puces, boutons, attaques invasives. Cadres de normatifs en sécurité et en sûreté (frameworks). Responsabilité professionnelle : éthique et impacts. Vérification et tests. Modalités : cours de 3 heures et un laboratoire de 3 heures/semaine.

OBJECTIFS

- Ce cours vise à sensibiliser les étudiants aux différents aspects de la sûreté de fonctionnement et de la sécurité des systèmes embarqués. On développera les compétences nécessaires à la prise en charge des objectifs essentiels de sécurité et de sûreté. Spécifiquement, l'étudiant qui complète le cours avec succès sera capable :
- ❏ de définir les concepts importants en sûreté : fautes, défaillances, erreurs, fiabilité, disponibilité;
- ❏ de distinguer les paramètres probabilistes utilisés en fiabilité : MTTF, MTTR, MTBF;
- ❏ d'expliquer certaines techniques permettant d'améliorer la fiabilité : évitement, tolérance, suppression de fautes;
- ❏ de mettre en oeuvre des mécanismes visant à assurer la fiabilité et la sécurité des systèmes;
- ❏ de définir et mettre en contexte les principaux objectifs et services de sécurité, tels que confidentialité, intégrité, authentification;
- ❏ d'expliquer la fonction des principaux mécanismes de sécurité : chiffrage, hachage, signature;
- ❏ d'expliquer la fonction de protocoles cryptographiques courants utilisés en sécurité;
- ❏ de reconnaître les vulnérabilités de systèmes.

ÉVALUATION

Description sommaire	Date	Pondération
Devoirs		10 %
Travaux pratiques	Spécifiée dans les énoncés	40 %
Examen final	Fin du trimestre	50 %

Devoirs

Occasionnellement au cours de la session, des séries d'exercices à réaliser en devoir seront soumises aux étudiants. Typiquement, il y a deux devoirs avec environ deux semaines entre la soumission et la remise. Un sous-ensemble (inconnu à l'avance) des exercices pourra être retenu pour être noté. Les énoncés des devoirs seront distribués par l'intermédiaire de Moodle. Il n'y a pas de format pré-établi pour les documents à remettre, mais la qualité de présentation et de rédaction est importante. Une réponse ou un raisonnement illisible est forcément mauvais.

Travaux pratiques

La mise en pratique des concepts vus en classe se fera par la réalisation de travaux pratiques en laboratoire, faisant appel à différents environnements de développement et de simulation. Ces travaux seront réalisés par équipes de quelques étudiants.

Remise des rapports

Les devoirs et rapports doivent être rendus électroniquement par l'intermédiaire du site Moodle du cours. Les travaux remis en retard seront pénalisés, à raison de 20 % de la note globale par jour (incluant samedi, dimanche et congés) de retard. Exceptionnellement (par ex., panne de Moodle), une copie pourra être rendue par courriel régulier.

Chaque fichier doit être nommé de façon à ce qu'on puisse identifier les membres de l'équipe (par exemple, par l'utilisation d'initiales), de même que le titre de la manipulation / simulation. Si plusieurs versions d'un même rapport sont remises, un numéro de version significatif doit être inclus dans le nom. Attention : des erreurs de titres pourraient faire que des copies ne soient pas corrigées, ou que des résultats soient confondus par mégarde.

Le format de fichier pour les documents doit **absolument** être pdf (Portable Document Format), ce qui assure que ce qui est rendu est conforme à la version de l'étudiant et ne risque pas d'être modifié par la suite. Un rapport doit normalement être présenté en un seul fichier, avec annexes, le cas échéant, pour les codes sources, etc. Un

guide détaillé disponible sur le site du cours, donne davantage d'informations sur la présentation des rapports de laboratoire.

Les règlements concernant le plagiat seront strictement appliqués. Pour plus de renseignements, veuillez consulter le site suivant :

http://www.sciences.uqam.ca/etudiants/integrite-academique.html

Examen

Une moyenne d'au moins 50 % à l'examen est exigée pour réussir le cours.

L'utilisation de documentation personnelle (notes de cours, manuels) à l'examen sera limitée à quelques pages de notes personnelles.

Politique d'absence aux examens

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 : **http://info.uqam.ca/politiques/**

L'étudiant-e doit déposer le formulaire dûment complété au secrétariat de la direction de son programme d'études : SH-4700 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 : **http://info.uqam.ca/politiques**

CONTENU

❑

- Les problématiques de la sécurité et de la sûreté des systèmes embarqués. Définitions, distinctions, objectifs, renforcement mutuel, antagonisme. Malveillant, accidentel. Préjudices, dommages. Fiabilité, confiance. Risques malveillants ou accidentels.
- Objectifs de sécurité; confidentialité, intégrité, disponibilité, authentification, non-répudiation, contrôle d'accès. Vulnérabilités, menaces à la sécurité et attaques.
- Attaques conduisant à des fuites d'information, à des modifications d'information, à des privations de service. Attaques passives et actives. Attaques spécifiques contre les systèmes embarqués : piratage, ingénierie inversée, clonage. Sécurité des réseaux de capteurs.
- Techniques de base en sécurité. Techniques de chiffrage. Mécanismes de base : transposition, permutation. Caractérisation des systèmes de chiffrage.
- Mécanismes sécuritaires modernes : systèmes de chiffrage symétriques et asymétriques. Complexité de calcul. Fonctions à sens unique. Hachage cryptographique. Intégrité des données et authentification de message. Génération pseudo-aléatoire. Modes de chiffrage : en blocs, continu, chaînage de blocs chiffrés.
- Protocoles sécuritaires : identification et authentification. Protocoles : signature, authentification mutuelle. Échange et gestion de clés. Tiers de confiance. Authentification par défi et réponse. Protocoles sans transfert de connaissances. Infrastructures d'authentification et de distributions de clés. Certificats.
- Sécurité des plateformes embarquées : circuits programmables, amorçage sécuritaire, mécanismes matériels sécuritaires.
- Problématique de la sûreté des systèmes embarqués. Causes : fautes, défaillances, erreurs.
- Fiabilité de système, de matériel, de logiciel : MTTF, MTTR, MTBF.
- Critères de sûreté de fonctionnement : fiabilité, disponibilité, innocuité, maintenabilité, testabilité.
- Mécanismes de contrôle : tolérance aux fautes, suppression des fautes, conception pour la fiabilité.

- Modélisation de la sûreté et de la sécurité. Arbres de défaillance, d'attaques, de menaces.

RÉFÉRENCES

V R Schneier, B. – *Cryptographie appliquée, 2e édition* – **1996.**

V C Stinson, D.R. – *Cryptographie, Théorie et Pratique* – **1995.**

V C Zémor, G. – *Cours de cryptographie* – **2000.**

V C Pfleeger, C.P. – *Security in Computing* – **2002.**

V C Motet, G. – *Sûreté de fonctionnement des systèmes informatiques* – **1998.**

V C *Handbook of Software Reliability Engineering* – **IEEE Computer Society Press. 1996.**

V C Siewiorek & Swarz – *Reliable Computer Systems : Design and Evaluation* – **1992.**

V C Musa, Iannino & Okumoto – *Software Reliability : Measurement, Prediction, Application* – **1990.**

V C *Software Reliability Handbook* – **Elsevier Applied Sciences. 1990.**

V C Sabnis – *VLSI Reliability* – **1990.**

V C Stapko, T. – *Practical Embedded Security* – **2008.**

V C Çayirci, E., Rong, C. – *Security in Wireless Ad Hoc and Sensor Networks* – **2009.**

V C Dargie, W. & Poellabauer, C. – *Fundamentals of wireless sensor networks: theory and practice* – **2010.**

V C Shelby, Z. & Bormann, C. – *6LoWPAN: The Wireless Embedded Internet* – **2007.**

V C Elahi, A. – *ZigBee Wireless Sensor and Control Network* – **2010.**

U O **http://www.moodle,uqam.ca**
Site web du cours via Moodle

AUTRES LECTURES

D'autres documents seront soumis pour lecture durant la session. La liste sera tenue à jour sur Moodle.

A : article – C : comptes rendus – L : logiciel – N : notes – R : revue – S : standard – U : uri – V : volume

C : complémentaire – O : obligatoire – R : recommandé