Matière : Modélisation des Systèmes Communicants (MOD.SYS.COM)

Semestre : S3 / Unité d'enseignement : UEM 3.2

Crédits : 3 / Coefficient : 3

Objectifs de l'enseignement :

Les compétences développées dans le cadre de ce cours sont :

- *Apprendre les langages de spécification formelle,*
- *décrire formellement de systèmes communicants,*
- *appliquer les techniques de modélisation aux protocoles de sécurité,*
- *exprimer les propriétés à satisfaire par les systèmes communicants,*
- *apprendre à appliquer les techniques de vérification formelle.*

Connaissances préalables recommandées :

- *Génie Logiciel*
- *Théorie des Langages.*

Contenu de la matière (1 cours, 1 TD par semaine) :

1. *Introduction aux Méthodes Formelles*
 - *Notions de Base*
 - *Processus de Modélisation*
 - *Langages Formels de Description de Systèmes*
 - *Techniques Formelles de Vérification*
2. *Algèbre de Processus CSP*
 - *Syntaxe*
 - *Système de Transitions*
 - *Sémantique Opérationnelle*
3. *Sémantique Dénotationnelle des traces CSP*
 - *Modèles des traces*
 - *Relation de satisfaction*
 - *Raffinement de traces*
 - *Modèles des failures*
4. *Modélisation des Protocoles de Sécurité en CSP*
 - *Modèles de protocoles fiables*
 - *Types de données pour les modèles de protocole*
 - *Modélisation de l'intrus*
5. *Spécification des Propriétés des Protocoles de Sécurité*
 - *Confidentialité*
 - *Authentification*
6. *Spécification à base de réseau de Petri : Security Protocol Language (SPL)*
 - *Syntaxe*
 - *Sémantique*

Type d'évaluation :

- *Contrôle continu*
- *Examen semestriel final*

Références (Livres et polycopiés, sites internet, ..., etc) :

- *Modelling and Analysis of Security Protocols, by Peter Ryan (Author), Steve Schneider (Author), Michael Goldsmith (Author), Gavin Lowe (Author), Bill Roscoe (Author), Addison Wesley; 01 edition (6 Dec. 2000) .*
- *C. A. R. Hoare, Communicating Sequential Processes, Prentice-Hall, Inc., USA, 1985, ISBN:0-13-*

153271-5 .

- *Roland Bouroulet, Raymond Devillers, Hanna Klaudel, Elisabeth Pelz, et Franck Pommereau. Modeling and analysis of security protocols using role based specifications and Petri nets. Dans , volume 5062 de Lecture Notes in Computer Science, pages 72-91, 2008.*
- *Bouroulet, R. and Klaudel, H. and Pelz, E. Semantics of Security Protocol Language (SPL) using a class of composable high-level Petri nets, Technical Report TR-2004-01, LACL, Université Paris 12 Créteil.*