USRS2G - Sécurité et sûreté de fonctionnement l'embarqué mobile avancées

Mis à jour le 29-05-2017

Code : USRS2G

Unité spécifique de type cours

5 crédits

Responsabilité nationale :
EPN05 - Informatique / 1

Contact national :

EPN05 Informatique

2 rue conté
31.1.79
75003 Paris
01 40 27 22 58
Swathi RANGANADIN RAJASELVAM
swathi.rajaselvam@lecnam.net

Présentation

Objectifs pédagogiques

Etude des problèmes de sécurité et sûreté de fonctionnement rencontrés dans les systèmes embarqués.

Programme

Contenu

Présentation approfondie des techniques de cryptographie et des protocoles réseau pour obtenir des propriétés de sécurité désirées. Nous sensibiliserons les étudiants par la présentation de quelques attaques algébriques et des attaques sur les protocoles pour en dégager des grands principes de design des protocoles sécuritaires. Nous présenterons les efforts de formalisation et de certification des politiques de sécurité. Le cours sera complété par des interventions plus spécifiques :

- Nous présenterons les travaux sur la détection d'intrusion dans les domaines dans l'embarqué en particulier dans les réseaux de capteurs.
- Nous présenterons les problèmes de sécurité dans le domaine des RFIDs,..
- Nous parlerons aussi de la formalisation des politiques de sécurité et leur certification à l'aide d'assistants de preuve. Dans le même esprit nous présenterons l'utilisation de model-checker pour la vérification des politiques de sécurité.
- Nous aborderont la détection statique des canaux cachés dans les compilateurs (bien sur ce n'est pas spécifique des systèmes embarqués, mais c'est essentiellement dans ce domaine que les gens se sont penchés sur la question . . .) Pour la partie sûreté de fonctionnement, on insistera sur la mise en oeuvre des méthodes présentées dans l'UE STAP et de leur utilisation conjointe dans le cadre des normes définissant les familles des métiers de l'embarqué.
- Évitement des erreurs de conception logicielle : méthodes de spécification formelle, langages formels et preuve, processus de développement formel, approche B, approche synchrone, langages d'expression et de vérification de propriétés.
- Détection des erreurs d'exécution : analyse statique fondée sur l'interprétation abstraite, techniques d'élimination des erreurs (AEEL, règles de codage et de relecture critique de code), test. - Processus de développement de systèmes sûrs à logiciel prépondérant : caractérisation des exigences, choix d'architecture, choix au niveau du logiciel, logiciels off the shelf, démarche constructive, traçabilité du profil sûreté de fonctionnement.