Séminaire Axe

Génie des Logiciels et des Systèmes d'Information

9 mai 2017

Matin - Salle 206

10H30 : Salvador MARTINEZ PEREZ - Model-driven engineering for ICT access-control configuration analysis

Access-control policies constitute a widespread mechanism for the implementation of the Confidentiality and Integrity security properties in ICT Systems. In this sense, means to provide access-control configurations are integrated in many different systems. Firewalls, RDBMSs or web applications, among others, are examples of Systems integrating access-control mechanisms. Unfortunately, the configuration and/or manipulation of an access-control policy by using such provided capabilities remains a difficult and error prone task that requires a high level of expertise where vendor-specific concrete syntaxes and semantics must be mastered. While approaches based on formal refinement techniques, e.g., using abstract machines grounded on the use of set theory and first order logic have been proposed to ensure, by construction, cohesion and correctness of access-control policies, their adoption in real systems remains scarce as they normally demand skills not necessarily common among security experts (such as set theory, etc) and moreover, do not provide the means to fill the gap between an existing configuration and the formalism. Conversely, Model-driven engineering and its ability for the reduction of system's complexity by the means of abstraction and integration comes out as an ideal solution in order to 1) ease the analysis and management of access-control policies and 2) fill the gap between existing configurations and the analysis tasks. Concretely, model-driven engineering tools and techniques can be used in order to obtain higher level representations of access-control policies where the essential security information is kept, provide re-usable analysis tasks and re-generate corrected and/or re-factored vendor-specific configurations.

Après-midi – Amphi

13H : Frederico ALVARES (en visioconférence) - L'informatique autonomique pour les systèmes logiciels répartis et les perspectives pour l'auto-protection

Dans cet exposé, je vais aborder mes travaux de recherche autour de l'auto-adaptation des systèmes logiciels répartis à large échelle. Ces travaux s'appuient fortement à la fois sur : (i) des techniques de génie logiciel (langages dédiés, modèles, architectures), lesquelles facilitent la définition et la manipulation de ce type d'applications; (ii) des méthodes formelles, permettant d'avoir des garanties sur leur comportement à l'exécution; (iii) des plateformes réelles d'exécution allant des intergiciels pour les composants logiciels reconfigurables jusqu'à des grandes infrastructures de calcul comme Grid'5000 et des plateformes Cloud telles que OpenStack. Ensuite, je présenterai mon projet d'intégration au LIG, en particulier je parlerai des perspectives de l'utilisation de l'informatique autonomique dans le contexte sécuritaire des applications, c'est à dire, des problématiques et pistes de recherche potentielles liées à la mise en en place de l'auto-protection dans les applications logicielles.

13H45 : Vanea CHIPRIANOV - Modélisation des architectures sécurisés des systèmes à prépondérance logicielle

Cette présentation donnera un aperçu de mes travaux de recherche, centrés sur les activités de conception et simulation des architectures de systèmes et des entreprises (par exemple basés sur SOA ou encore TOGAF). Nous verrons des propositions des langages de modélisation (dans le sens IDM) spécifiques aux domaines des systèmes de télécommunications, sous-marins et systèmes-de-systèmes (ville/bâtiment intelligent en particulier). Ces langages ont des fortes caractéristiques collaboratives (capture du "design rationale"), de performance et de sécurité (contrôle d'accès - OrBAC, attaques en cascades). Elles sont complétés par des processus et méthodes qui décrivent leur utilisations dans des équipes collaboratives. Je finirai par présenter mon projet d'intégration dans le LIG, en premier lieu dans l'équipe SIGMA (par exemple dans le projet SmartRoad), mais avec des possibles riches interactions avec d'autres équipes aussi.

14H30 : Nghi HUYNH - Vérification de politiques de contrôle d'accès avec gestion du consentement dans le domaine médical

Dans le domaine médical, la numérisation des documents et l'utilisation des dossiers patient électroniques (DPE, ou en anglais EHR pour Electronic Health Record) offrent de nombreux avantages, tels que la facilité de recherche et de transmission de des données. Les systèmes informatiques doivent reprendre ainsi progressivement le rôle traditionnellement tenu par les archivistes, rôle qui comprenait notamment la gestion des accès à ces données sensibles. Ces derniers doivent en effet être rigoureusement contrôlés pour tenir compte des souhaits de confidentialité des patients, des règles des établissements et de la législation en vigueur. SGAC, ou Solution de Gestion Automatisée du Consentement, a pour but de fournir une solution dans laquelle l'accès aux données du patient serait non seulement basée sur les règles mises en place par le patient lui-même mais aussi sur le règlement de l'établissement et sur la législation. Cependant, cette liberté octroyée au patient est source de divers problèmes : conflits, masquage des données nécessaires aux soins ou encore tout simplement erreurs de saisie. Pour effectuer ces vérifications, les méthodes formelles fournissent des moyens fiables de vérification de propriétés tels que les preuves ou la vérification de modèles.
Nous proposerons des méthodes de vérification adaptées à SGAC pour le patient : introduction du modèle formel de SGAC et des méthodes de vérifications de propriétés. Afin de mener ces vérifications de manière automatisée, SGAC est modélisé en B et Alloy ; ces différentes modélisations donnent accès aux outils Alloy et ProB, et ainsi à la vérification automatisée de propriétés via la vérification de modèles ou model checking.

15H15 : Hande Alemdar – Human activity recognition in smart homes with multiple residents

Recognizing human behavior in an automated manner is essential in many ambient intelligence applications such as smart homes, health and well-being monitoring and emergency response services. In smart environments equipped with tiny sensors that can measure the interactions between the residents and the environment, human activities can be recognized using machine learning techniques. Most of the existing methods, however, consider a single person living inside a smart house. The studies that can handle the multiple residents generally assume a location identification mechanism such as RFID that allows the system to differentiate between the sensor readings for each resident. Both of these assumptions are too restrictive that they prevent the general applicability of activity recognition systems. In this talk, we will focus on making smart houses smart enough to provide long term health monitoring for not only people who live alone but also with a spouse or a flat mate. Our goal is recognizing the individual's behavior in multi-resident environments without assuming any person identification which generally requires the use of obtrusive wearable technology. We propose two approaches for handling the multiple-resident case. First, we directly model the overlaid observations together with multiple chains of activity sequences using a factorial hidden Markov model (FHMM) model. Secondly, we use nonlinear Bayesian tracking for decomposing the observation space into the number of residents. For each method, we perform experimental evaluation on real-world data sets and discuss the advantages and disadvantages.

16H : Mario CORTES CORNAX – Amélioration Continue des Systèmes d'Information et Implications sur la Sécurité

Mes travaux concernent la conception et l'analyse de systèmes d'information complexes, avec une approche d'ingénierie dirigée par les modèles. Je m'intéresse notamment aux processus métiers supportés par les systèmes d'information, qui se tournent vers l'automatisation. La prise en compte de certains aspects organisationnels (ex. processus collaboratifs) et sociaux (ex. les interaction humaines avec le système) représentent encore des défis importants pour l'automatisation ainsi que dans la prise en compte de la dimension sécuritaire. Dans ce cadre, mes contributions concernent une approche dirigée par les modèles, centrée utilisateur et supportée par des méthodes d'amélioration continue pour aider à la compréhension, la conception, et la mise en place de ce type de systèmes complexes. Dans la continuité de ces travaux, mon projet de recherche vise à l'intégration des besoins en matière de sécurité au sein d'un cycle d'amélioration continue.