Friday 10 November 2017
10h30
UT3 Paul Sabatier, IRIT, Auditorium J. Herbrand

Anas MONTII
Team MACAO - IRIT

Ingénierie des architectures logicielles sécurisées : patrons, modèles et analyses

Jury:
Antonio Manã – Professeur à l'Université de Malaga, Rapporteur,
Laurent PAUTET – Professeur à TelecomParis, Rapporteur,
Abdelmalek BENZEKRI – Professeur à l'Université Paul Sabatier,
Jean-Michel BRUEL – Professeur à l'Université Toulouse Jean-Jaurès,
Yves ROUDIER – Professeur à l'Université de Nice Sophia Antipolis,
Brahim HAMID – Maître de conférences à l'Université Toulouse Jean-Jaurès, Directeur de thèse,
Agnès LANUSSE – Ingénieur Chercheur au CEA LIST, Codirectrice de thèse
Claire PAGETTI – Ingénieur Chercheur à l'ONERA

Keywords: ICT, Security Engineering, Risk Assessment, Pattern-Based System Engineering (PBSE), Security patterns, Model-Driven Engineering (MDE), UML

Abstract: Nowadays most organizations depend on Information and Communication Technologies (ICT) to perform their daily tasks (sometimes highly critical). However, in most cases, organizations and particularly small ones place limited value on information and its security. In the same time, achieving security in such systems is a difficult task because of the increasing complexity and connectivity in ICT development. In addition, security has impacts on many attributes such as openness, safety and usability. Thus, security becomes a very important aspect that should be considered in early phases of development. In this work, we propose an approach in order to secure ICT software architectures during their development by considering the aforementioned issues. The contributions of this work are threefold: (1) an integrated design framework for the specification and analysis of secure software architectures, (2) a novel model- and pattern-based methodology and (3) a set of supporting tools.

The approach associates a modeling environment based on a set of modeling languages for specifying and analyzing architecture models and a reuse model repository of modeling artifacts (security pattern, threat and security property models) which allows reuse of capitalized security related know-how. The approach consists of the following steps: (a) model-based risk assessment performed on the architecture to identify threats, (b) selection and instantiation of security pattern models towards the modeling environment for stopping or mitigating the identified threats, (c) integration of security pattern models into the architecture model, (d) analysis of the produced architecture model with regards to other non-functional requirements and residual threats. In this context, we focus on real-time constraints satisfaction preservation after application of security patterns. Enumerating the residual threats is done by checking techniques over the architecture against formalized threat scenarios from the STRIDE model and based on existing threat references (e.g., CAPEC).
As part of the assistance for the development of secure architectures, we have implemented a tool chain based on SEMCO and Eclipse Papyrus to support the different activities based on a set of modeling languages compliant with OMG standards (UML and its profiles). The assessment of our work is presented via a SCADA system (Supervisory Control And Data Acquisition) case study.