Support for modelling and integration of reusable security building blocks in embedded systems

Maria Vasilevskaya and Simin Nadjm-Tehrani

Dept. of Computer and Information Science, Linköping University, Sweden
e-mail:[maria.vasilevskaya, simin.nadjm-tehrani]@liu.se

May 6, 2013

Abstract

Embedded devices are enablers of Internet of Things with countless applications. These devices store and manipulate sensitive information that is the target of sophisticated attacks. Thus, embedded systems must be protected against security threats. However, designing a secure embedded system is a difficult task, e.g., due to the tightly interdependence of security and resource constraint concerns. Model-Based Development (MBD) and Domain-Specific Modelling (DSM) are promoted to address complexity and ease the design of software-intensive systems. In our work, we leverage these two technologies to define a framework, which is an increment to existing methodologies for development of embedded systems, to assist a system engineer to systematically treat security issues within a system model. This framework is built on a premise that enforcement of separation of security and embedded system concerns is essential for efficient development of security-enhanced embedded system design. We achieve this goal defining techniques for both security and embedded system engineers to capture security knowledge in a particular domain and to reuse the knowledge when designing a system within different applications respectively.

In particular, security-specific knowledge relevant for a certain application domain is represented in a form of adapted information security ontology. The elements of the ontology are associated with security building blocks (models of security mechanisms) and their provided security properties. The selection of security building blocks to be integrated into a design of an embedded system is based on identification of a relevant subset of security properties retrieved from the captured security knowledge for a certain domain. The identification of relevant security properties is based on automatic elicitation of assets from the functional models of a system design and analysing vulnerabilities of an execution platform adopted by the embedded system engineer for a considered application. A tool is developed to support the proposed methodology and help to bridge between the security and embedded system domains. We illustrate our approach with a case study from the smart metering domain.