Chapter 96
Towards Test-Driven and Architecture Model-Based Security and Resilience Engineering

Ayda Saidane
University of Luxembourg, Luxembourg

Nicolas Guelfi
University of Luxembourg, Luxembourg

ABSTRACT

The quality of software systems depends strongly on their architecture. For this reason, taking into account non-functional requirements at architecture level is crucial for the success of the software development process. Early architecture model validation facilitates the detection and correction of design errors. In this research, the authors are interested in security critical systems, which require a reliable validation process. So far, they are missing security-testing approaches providing an appropriate compromise between software quality and development cost while satisfying certification and audit procedures requirements through automated and documented validation activities. In this chapter, the authors propose a novel test-driven and architecture model-based security engineering approach for resilient systems. It consists of a test-driven security modeling framework and a test based validation approach. The assessment of the security requirement satisfaction is based on the test traces analysis. Throughout this study, the authors illustrate the approach using a client server architecture case study.

INTRODUCTION

The concept of resilience was introduced in ICT systems in 1970s (Black 1976) and has been more intensively used in the research community in the very last years. By analyzing this research, we can notice that the word is used with many different definitions and at different levels (Black et al. 1997, Mostert et al., 1995, Ries, 2009, Górski et al., 2006). In (Guelfi 2011), we proposed a formal framework called DREF (Dependability and Resilience Framework) for modeling and evaluating resilient and dependable systems. In particular, it quantitatively defines resilience and satisfaction against

DOI: 10.4018/978-1-4666-4301-7.ch096

some functional or non-functional properties of interest. In our case, we focus on the evaluation of the security requirements satisfaction at both design and deployment phases. Specifically, we are designing a novel architecture-model based security testing methodology as an operational framework associated to DREF. In fact, we propose to use the interpretation of the test traces for experimentally evaluating the satisfaction of the security requirements by the system under test (SUT).

Model-driven engineering (MDE) is a software development methodology based on the usage, creation, validation and refinement of models representing that knowledge at different levels of abstractions from requirements to executable code. This methodology is gaining approval in industry especially in critical systems development with strong security and dependability requirements, because most of the MDE development process that is automated using model transformations appears to be less error-prone than classical methodologies. In our work, we are more specifically interested in security critical systems.

Software architecture design is an important step in the development process since it considerably impacts the quality of the system. An architectural model can be refined from the requirement phase where early model validation facilitates the detection and correction of design errors. This validation can be done either by formal verification or by testing. The architecture analysis is an activity that keeps running during the whole development process. What could be expected from testing the architecture model is the elicitation of attack scenarios exploiting some architecture level threats, like covert channels, and also lower level vulnerabilities by locating their activation and manifestation points. In addition, MDE-based development processes are based on successive model transformations from the architecture model to executable code. Consequently, we can consider that validating the system architecture model would be equivalent to validating the real system if the deployed model transformations and their automation are proved correct.

In this project, we are interested in security critical systems, which require a reliable validation process. So far, we are missing security-testing approaches providing an appropriate compromise between software quality and development cost and satisfying certification and audit procedures requirements through an automated and documented validation activities. In order to define such methodologies, we should explicitly and unambiguously define the threat and security requirements models and integrate this knowledge with the system architecture model in both design and validation phases. At design time, this knowledge influences the design choices since we must address these threats and equip the system with the necessary resources to mitigate them. At validation time, it is important to select test cases, covering both input models (requirements and threats), which correspond to potential security failures caused by malicious attacks or accidental security mechanisms failures.

We have selected the Architecture Analysis and Description Language (AADL)[1] as a modeling framework for our work. AADL is a SAE standard for system architecture description and analysis widely used in industry and supported by major avionics, automotive and telecommunications providers[2].

The chapter is structured as follows: section 2 presents the problem statements and the motivations; section 3 presents the basic concepts in DREF and overview of model based security testing state of the art; section 4 defines the running example; section 5 provides details on the proposed test-driven development process for robust secure systems.

MOTIVATIONS AND PROBLEM STATEMENT

Software architecture description languages provide a detailed view on the system's components, their interfaces and their interactions. We have