Abstract

Designing secure systems are a nontrivial task. Incomplete or faulty designs can cause security mechanisms to be incorrectly incorporated in a system, allowing them to be bypassed and resulting in a security breach. We advocate the use of the Aspect-Oriented Risk-Driven Development (AORDD) methodology for developing secure systems. This methodology begins with designers defining system assets, identifying potential attacks against them, and
evaluating system risks. When a risk is unacceptable, designers must mitigate the associated threat by incorporating security mechanisms methodically into the system design. Designers next formally evaluate the resulting design to ensure that the threat has been mitigated, while still allowing development to meet other project constraints. In this paper, we focus on the AORDD analysis, which consists of: 1) a formal security evaluation and 2) a trade-off analysis that enables system designers to position alternative security solutions against each other. The formal security evaluation uses the Alloy Analyzer to provide assurance that an incorporated security mechanism performs as expected and makes the system resilient to previously identified attacks.

Reference

- Verification and Trade-Off Analysis of security Properties in UML System Models (IEEE TRANSACTIONS ON SOFTWARE ENGINEERING, VOL. 36, NO. 3, MAY/JUNE 2010.)

Index Terms

Computer Science Ubiquitous Computing

Key words

Software Security AORDD