

SH-VT

METHODS AND TOOLS FOR ANALYZING AND DESIGNING SECURE SYSTEMS

Modern IT systems are often so complex that design faults don't become apparent until the software is run. By this point, costly redesign and delays, or even full system redevelopment, are just around the corner. The Fraunhofer Institute has developed methods and tools for the early detection, identification and better elimination of faults.

Executable models improve analysis options

The Fraunhofer Institute SIT supports system developers and software architects in the testing of functional requirements (Does the software do what it is supposed to do?) and helps answer non-functional questions (Does the system fulfill certain security properties?).

While conventional models such as UML only provide a static perspective of a system, the Fraunhofer Institute SIT uses methods and tools that enable the simulation and analysis of system variations, which is a major advantage. This allows to analyze the interaction between different system components and to better assess the effects of design decisions.

The versatile SH-Verification Tool

Fraunhofer's SH-Verification Tool is a powerful tool for modelbased analysis. It includes a simulator, a debugger and components for

verification and compact visualization of dynamic system behavior. The additional possibility of weighting individual actions enables risk and cost/benefit analyses, to name one example.

Focal point security

The Fraunhofer Institute SIT provides support in the evaluation and development of models throughout the entire development process. The objects of analysis are, among others:

- standards
- protocols
- architectures
- models and specifications
- communication interfaces

The focal points of the methods developed at the SIT are the verification of dynamic system attributes, in particular of the security aspects, and the testing of security requirements with respect to plausibility and consistency.

Target groups and applications

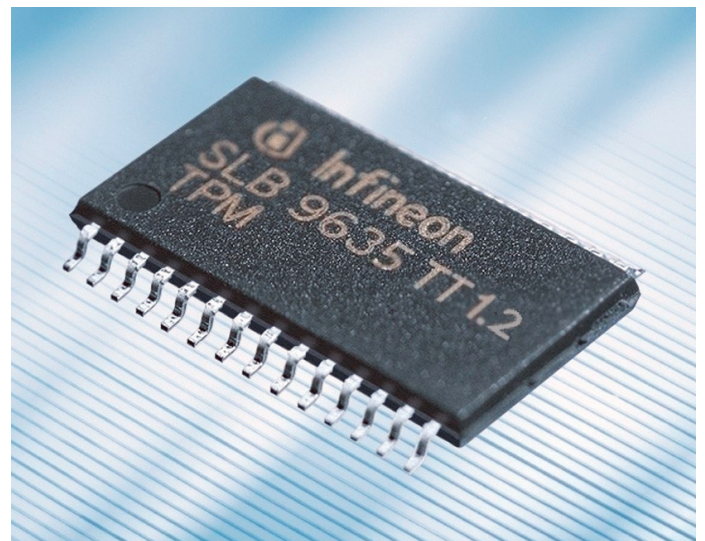
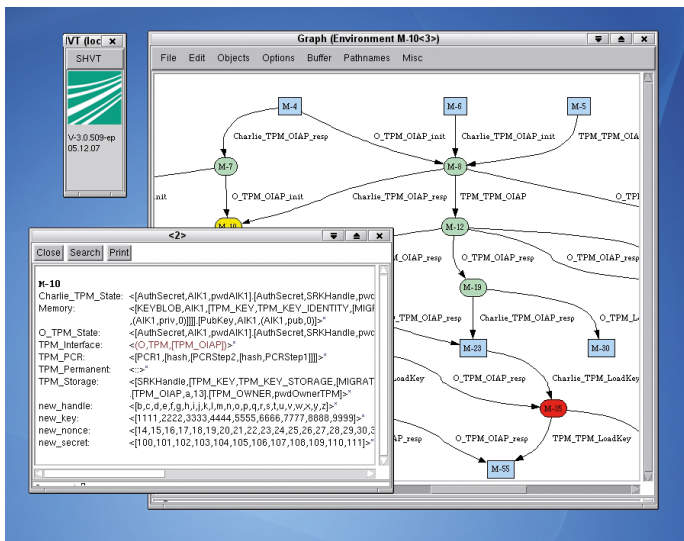
Model-based analysis is primarily geared towards:

- security agencies
- development departments
- research departments

*Fraunhofer Institute for Secure
Information Technology SIT*

*Contact:
Dipl.-Inform. Andreas Fuchs
Rheinstrasse 75
64295 Darmstadt, Germany*

*Phone +49 6151 869-228
Fax +49 6151 869-224
andreas.fuchs@sit.fraunhofer.de
www.sit.fraunhofer.de*



Current areas of application include test-case generation for smart cards, analysis involving the Trusted Platform Module (TPM) or web service and security policy analysis.

Reference projects

Valikrypt: Security analysis of cryptographic protocols for the German Federal Office for Information Security (BSI)

SicAri: Analysis of security policies for a security architecture for ubiquitous Internet use

Serenity: Design and validation of security patterns on network layers for policy-based selection of security mechanisms in Ambient Intelligence Systems.

Our offer

- We design and analyze security policies, security mechanisms and security models for business and management processes.
- We perform weak-point analyses and attack simulations.
- We formulate requirement profiles for system components.
- We analyze critical IT infrastructures.