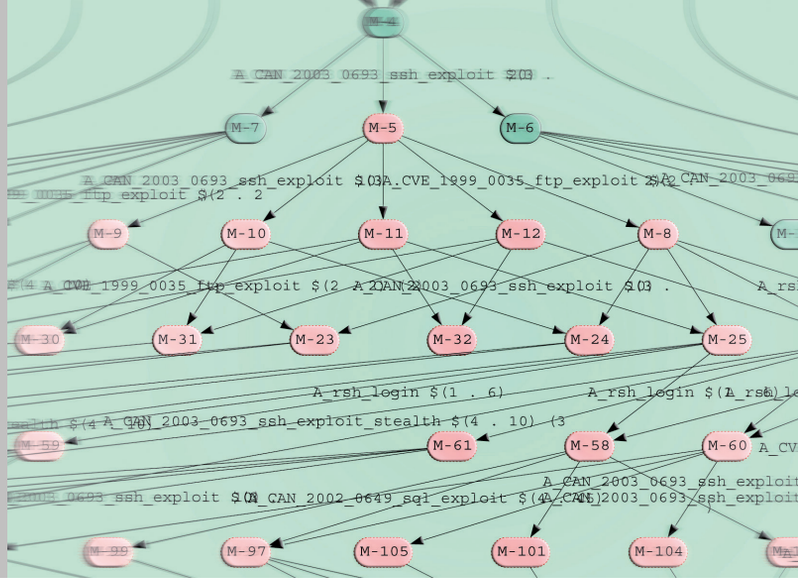
Fraunhofer
SIT

FRAUNHOFER-INSTITUT FÜR
SICHERE INFORMATIONSTECHNOLOGIE



SH-VT

METHODEN UND WERKZEUGE FÜR ANALYSE UND DESIGN SICHERER SYSTEME

Fraunhofer-Institut für Sichere Informationstechnologie SIT

Kontakt:
Dipl.-Inform. Andreas Fuchs
Rheinstraße 75
64295 Darmstadt

Telefon 06151 869-228
Fax 06151 869-224
andreas.fuchs@sit.fraunhofer.de
www.sit.fraunhofer.de

Heutige IT-Systeme sind oft so komplex, dass Designfehler erst beim Betrieb der Software auffallen. Dann drohen kostspielige Nachbesserungen und Verzögerungen oder gar die komplette Neu-Entwicklung. Das Fraunhofer-Institut SIT hat Methoden und Werkzeuge entwickelt, mit denen sich Fehler frühzeitig erkennen, exakt bestimmen und so besser beheben lassen.

Ausführbare Modelle verbessern Analyse-Möglichkeiten
Fraunhofer SIT unterstützt Systementwickler und Software-Architekten bei der Überprüfung funktionaler Anforderungen (Leistet die Software, was sie soll?) und hilft bei der Beantwortung nichtfunktionaler Fragen (Erfüllt das System Sicherheitseigenschaften?). Im Gegensatz zu herkömmlichen Modellen wie UML, die nur eine statische Sichtweise erlauben, nutzt das Fraunhofer-Institut SIT Methoden und Werkzeuge, mit denen sich Systemvarianten simulieren und analysieren lassen. Dadurch lassen sich die Wechselwirkungen verschiedener Systemkomponenten untersuchen und Auswirkungen von Designentscheidungen besser beurteilen.

Das SH-Verification Tool, ein vielseitiges Werkzeug
Mit dem SH-Verification Tool verfügt das Fraunhofer-Institut SIT über ein leistungsstarkes Werkzeug für die modellbasierte Analyse. Es enthält einen Simulator, einen Debugger sowie Komponenten zur Verifikation und kompakten Visualisierung des dynamischen Systemverhaltens. Die zusätzliche Gewichtung einzelner Aktionen ermöglicht zum Beispiel Risiko- und Kosten- / Nutzenanalysen.

Schwerpunkt Sicherheit
Das Fraunhofer-Institut SIT bietet Unterstützung in der Bewertung und Entwicklung von Modellen während des gesamten Entwicklungsprozesses. Gegenstand von Analysen sind unter anderem:

- Standards
- Protokolle
- Architekturen
- Modelle und Spezifikationen
- Kommunikationsschnittstellen

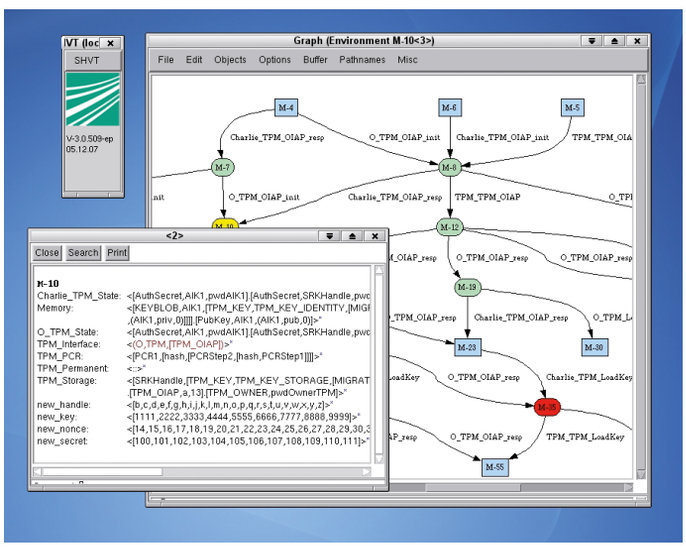
Der Schwerpunkt der am SIT entwickelten Methoden liegt dabei auf der Verifikation von dynamischen Systemeigenschaften, insbesondere von Security-Aspekten, sowie in der Überprüfung von Plausibilität und Widerspruchsfreiheit von Sicherheitsanforderungen.

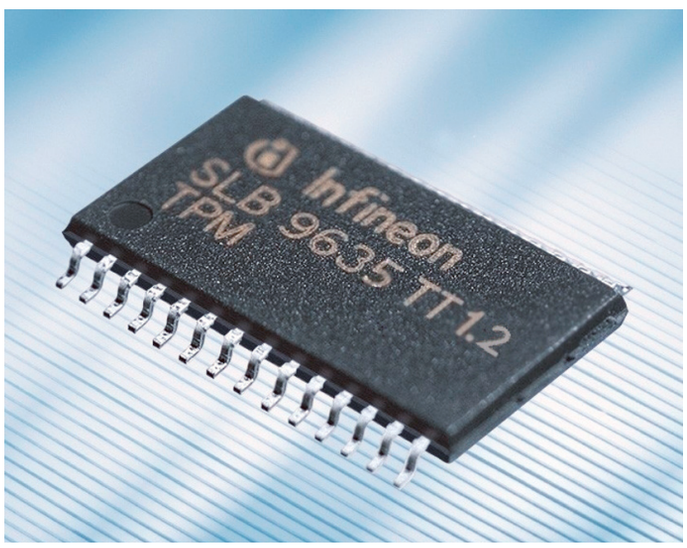
Zielgruppen und Anwendungen
Das Angebot zur modellbasierten Analyse richtet sich vor allem an:

- Sicherheitsbehörden
- Entwicklungsabteilungen
- Forschungsabteilungen

Anwendungsgebiete finden sich etwa in der Testfallgenerierung für Smartcards, in Analysen zum Trusted Platform Module (TPM) oder in Untersuchungen von Web Services und Sicherheitspolitiken.

11/2006





Referenzprojekte

Valikrypt: Sicherheitsanalyse kryptographischer Protokolle im Auftrag des BSI

SicAri: Untersuchung von Security Policies für eine Sicherheitsarchitektur für die ubiquitäre Internetnutzung

Serenity: Entwurf und Validierung von Security-Pattern auf Netzwerkebene zur policy-gesteuerten Auswahl von Sicherheitsmechanismen in Ambient Intelligence (AmI) Systemen

Unser Angebot

- Design und Bewertung von Security Policies, Sicherheitsmechanismen und Sicherheitsmodellen für Geschäfts- und Verwaltungsprozesse
- Schwachstellen-Analyse und Angriffssimulation
- Formulierung von Anforderungsprofilen an Systemteile
- Analyse kritischer IT-Infrastrukturen