A Cocoa GUI For The AVISPA Protocol Analyzer

Semesterarbeit WS05/06

Von: Natalie Trommer
Betreuer: Paul E. Sevinç
Paul Hankes Drielsma

Übersicht

- Aufgabenstellung
- AVISPA
- Cocoa
- Design
- Implementation
- Demo
- Fazit & future work
- Fragen

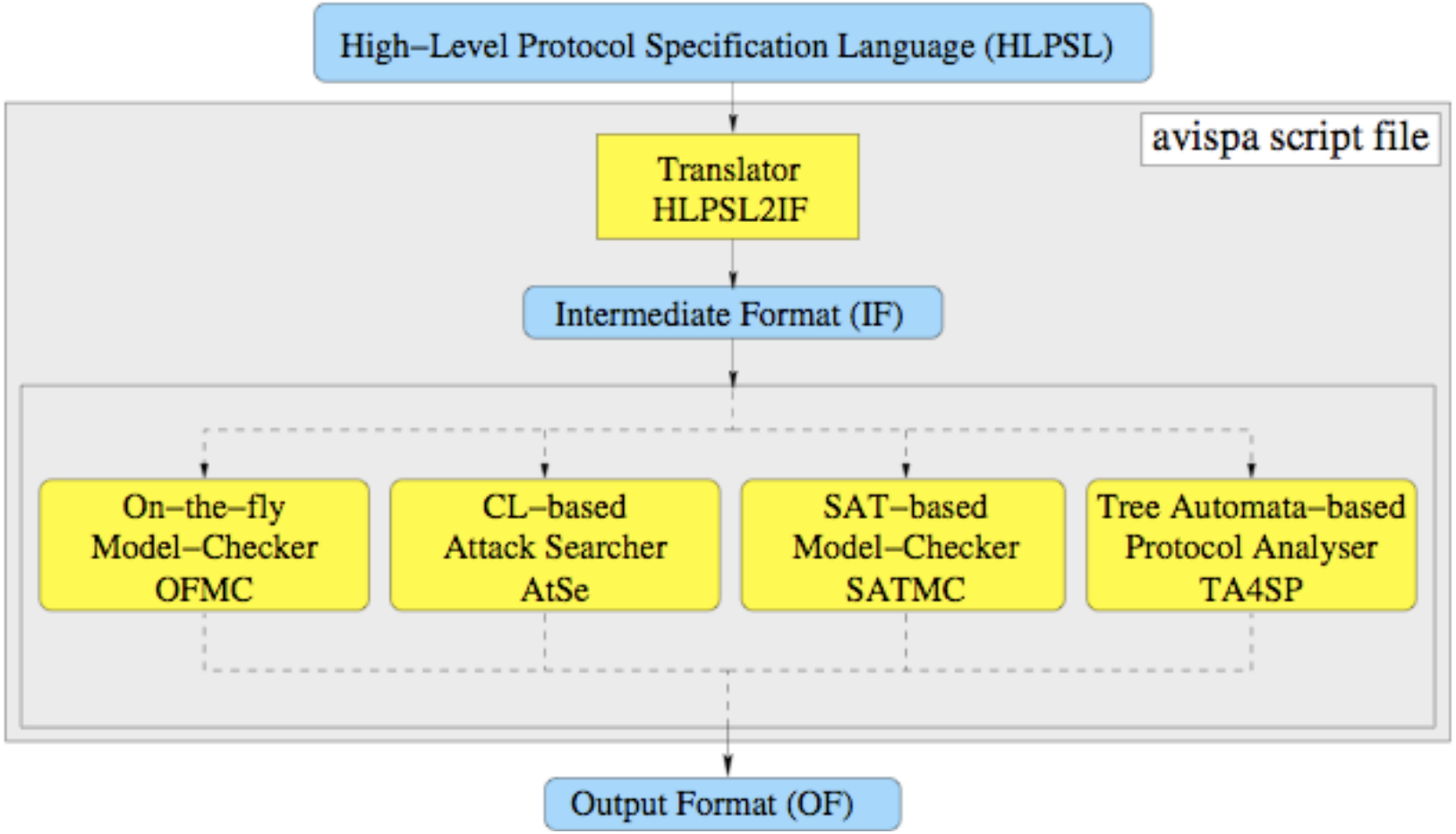
Aufgabenstellung

- Design und Implementation eines graphischen user interface für das AVISPA Tool
- Implementation:
  - Mac OS X
  - Cocoa application frameworks
  - Apple Human Interface Guidelines

AVISPA

- Automated Validation of Internet Security Protocols and Applications
- Tool um die Sicherheit von Internet-Protokollen und Anwendungen zu analysieren

AVISPA

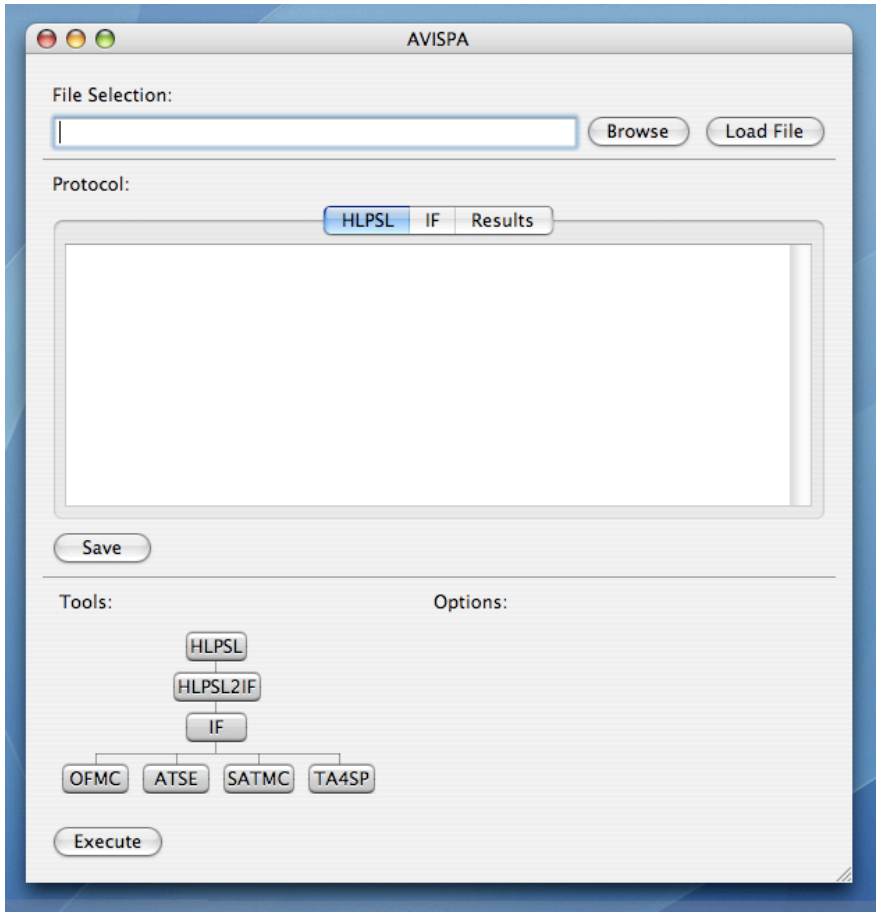

High–Level Protocol Specification Language (HLPSL)
avispa script file
Translator
HLPSL2IF
Intermediate Format (IF)
On–the–fly
Model–Checker
OFMC
CL–based
Attack Searcher
AtSe
SAT–based
Model–Checker
SATMC
Tree Automata–based
Protocol Analyser
TA4SP
Output Format (OF)

Cocoa application frameworks

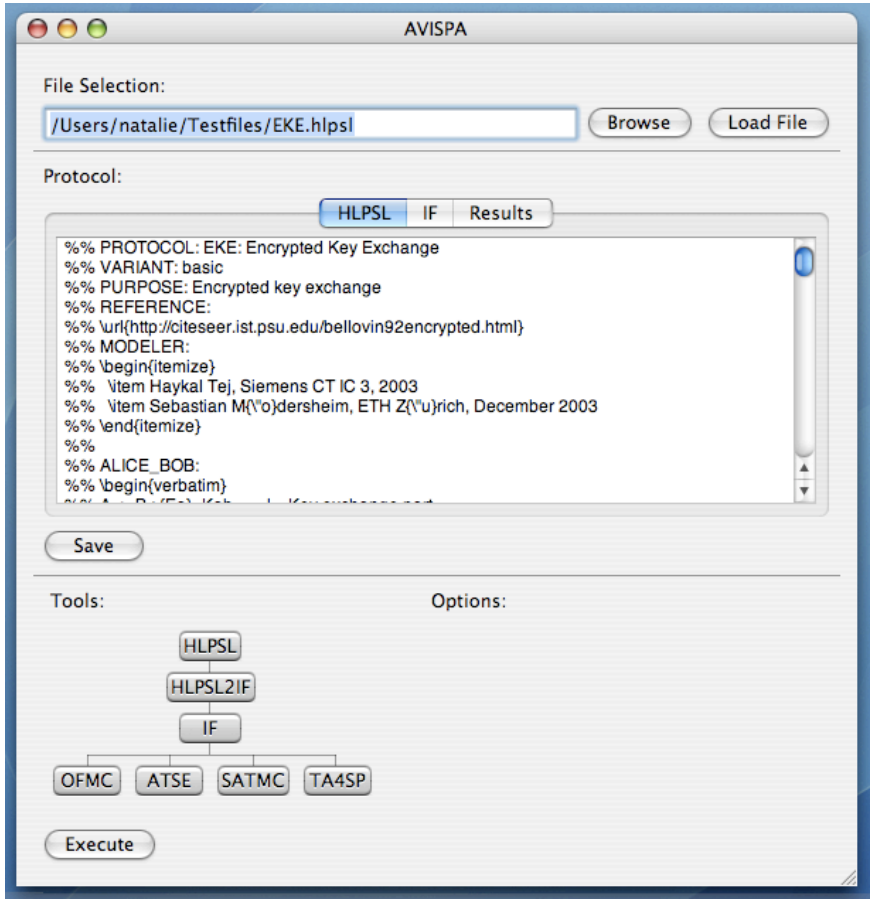
- Objekt-orientierte Entwicklungsumgebung für Mac OS X Applikationen
- Besteht aus mehreren objekt-orientierten Software Libraries und einer Runtime Engine
- Objective-C oder Java
- „Schnell & einfach“

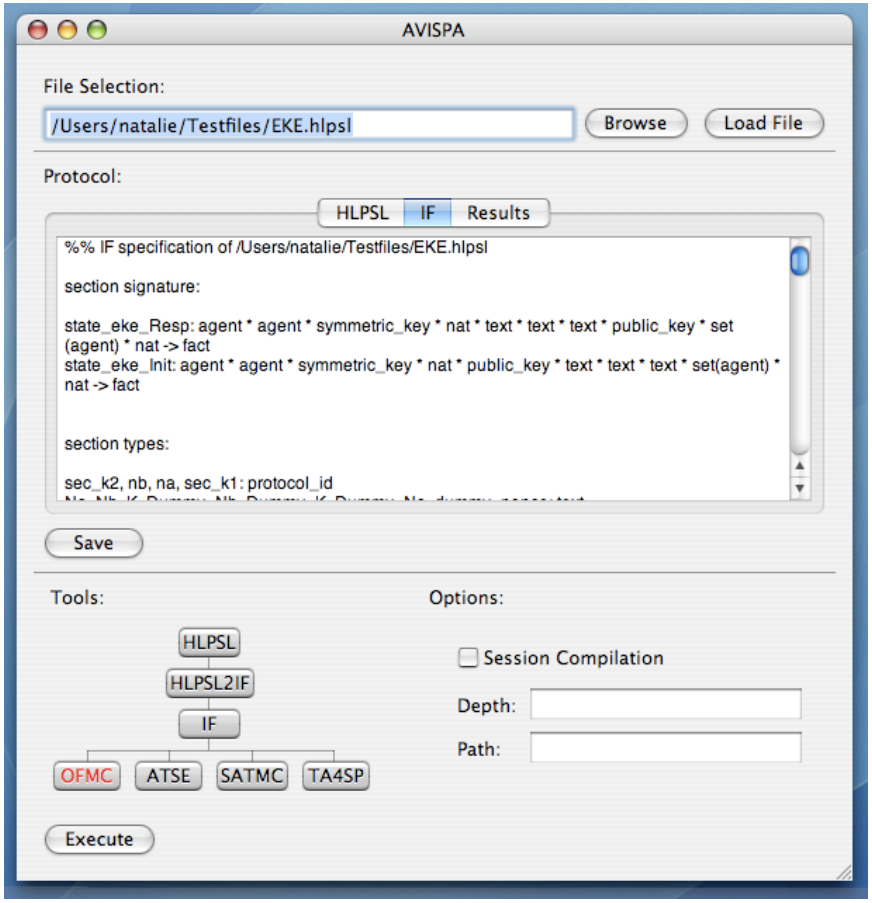
Design – Funktionalität & Aussehen

- hlpsl Files öffnen, editieren & speichern
- Tools ausführen & Optionen auswählen
- Resultate editieren & speichern



Design – Funktionalität & Aussehen



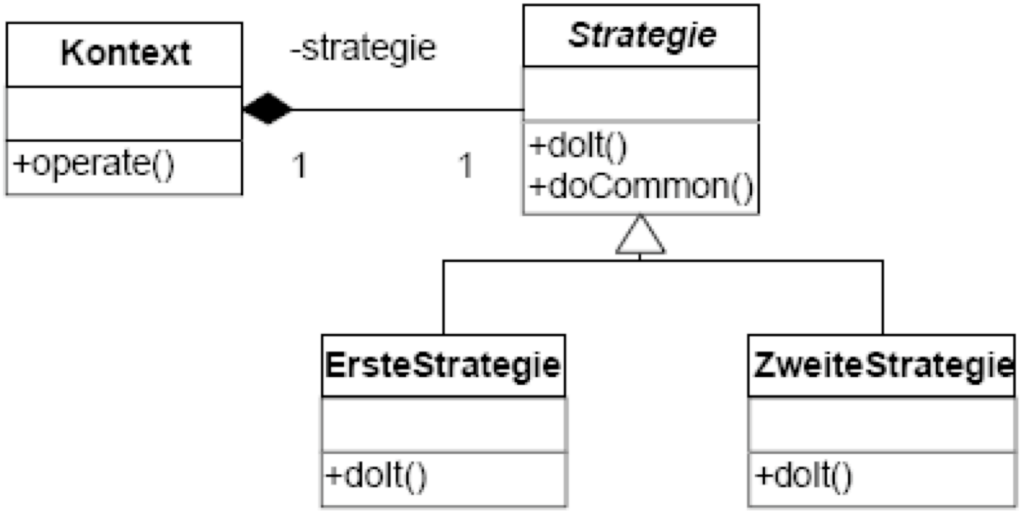


Design – Implementation

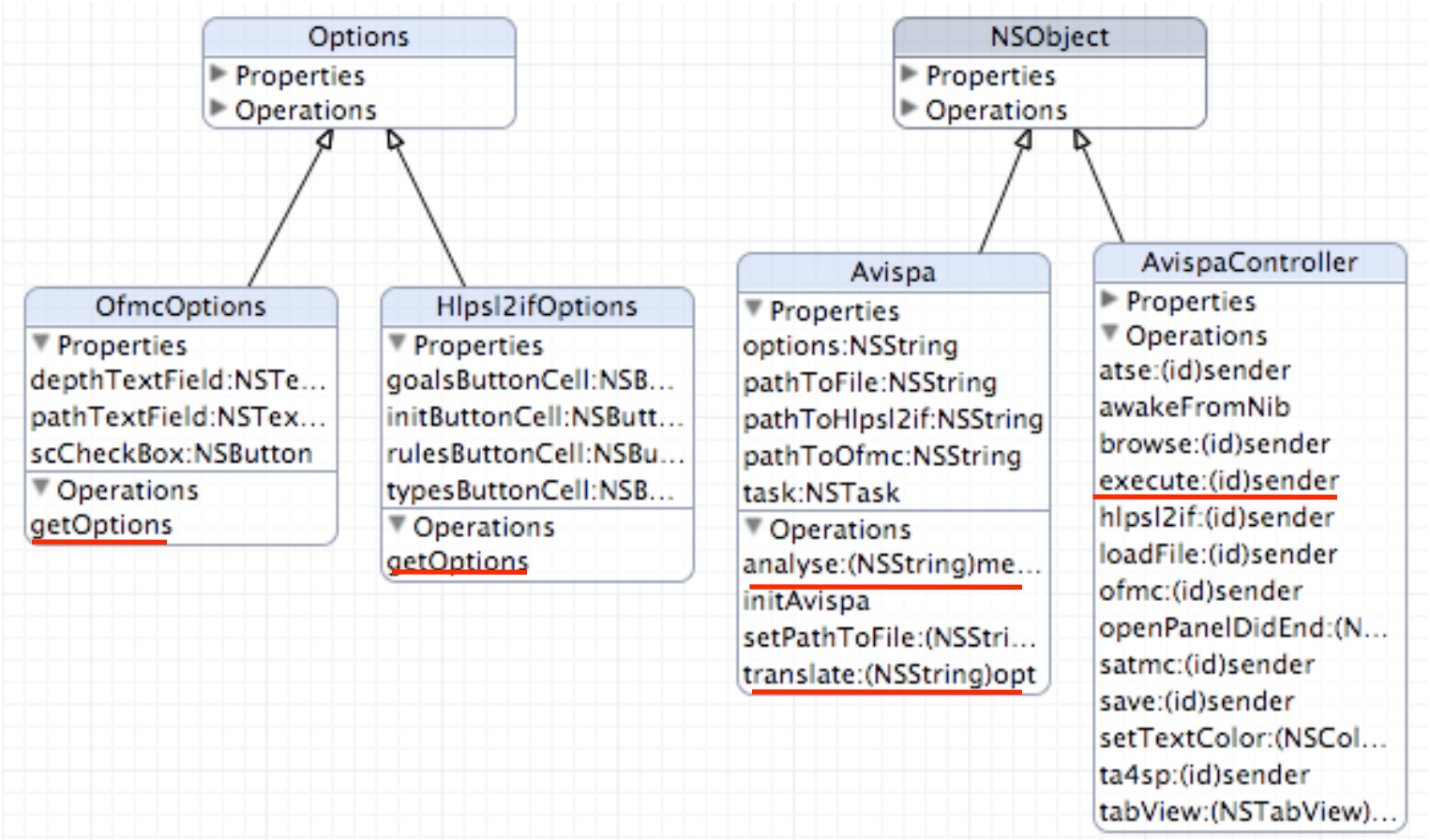
- Anforderung:
  So modular wie möglich, damit zukünftige Erweiterungen nur minimale Modifikationen benötigen
- Unterste Schicht AVISPA besteht aus vier Analysetools ...
- ... Lösung: Strategy-Pattern

Implementation – Strategy Pattern

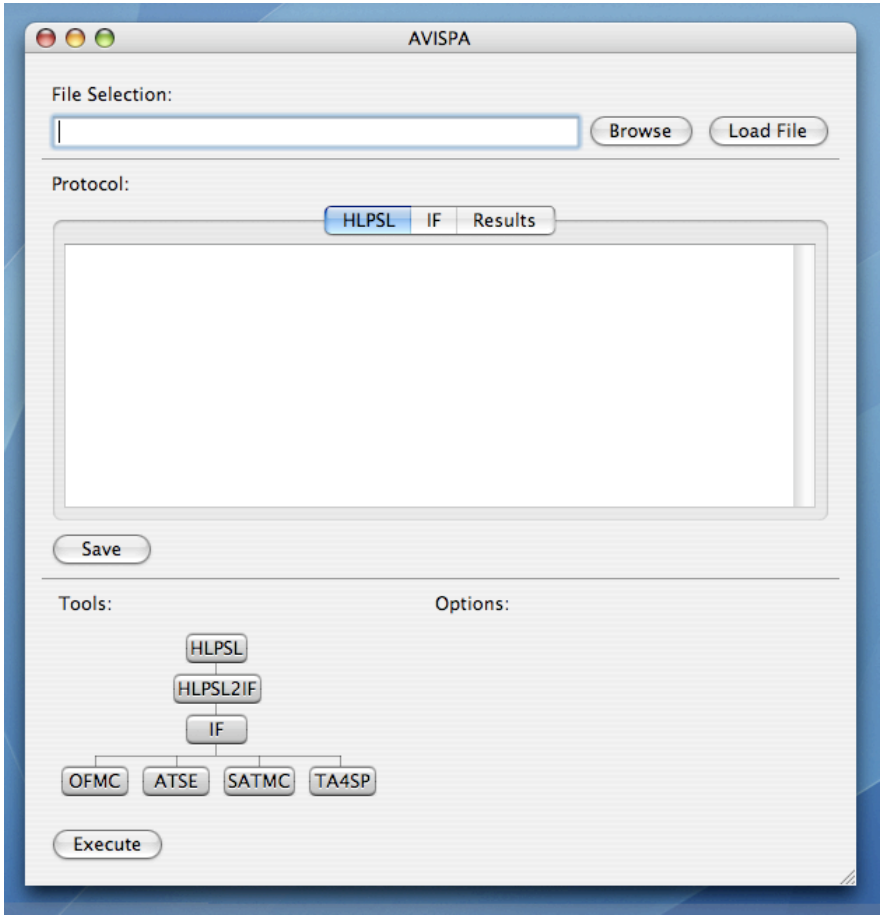
- Eine Kontext-Klasse kann auf verschiedene Versionen eines Algorithmus zugreifen



Implementation – Klassendiagramm



Demo


AVISPA
File Selection:
Browse
Load File
Protocol:
HLPSL
IF
Results
Save
Tools:
Options:
HLPSL
HLPSL2IF
IF
OFMC
ATSE
SATMC
TA4SP
Execute

Fazit & future work

- Spannende Arbeit
- ‘unbekanntes’ Mac OSX kennengelernt

- Resultate der Analyse:
  Text → Grafik: Message Sequence Chart
- Portieren der restlichen Analysetools

Fragen

???